VERIFICATION OF TRANSLATION

I, Toyoaki Fukui, translator of FUKUI & PARTNER of 1-19, Uchihonmachi 2-chome, Chuo-ku, Osaka-shi, Osaka, JAPAN, do hereby solemnly and sincerely declare as follows:

1. That I have a competent knowledge of the English and Japanese Languages.

2. That the attached document entitled:

"DATA MONITORING METHOD AND DATA MONITORING APPARATUS"

is a true and correct translation in English of a Japanese Patent Application No. 11-049997 filed on February 26, 1999.

DATED This 2nd day of June, 2003.

T. Fukui

Toyoaki Fukui
Translator

PATENT OFFICE

JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this office.

Date of Application: February 26, 1999

Application Number: Patent Application 11-049997

Applicant(s): Matsushita Electric Industrial Co., Ltd.

March 3, 2000

Commissioner,

Japan Patent Office Takahiko Kondoh

Certification No. 2000-3012825

[Document Name] Patent Request

[Docket Number] 2036610009

[Date of Filing] February 26, 1999

[Address] Commissioner of the Patent Office

[IPC] H04N 1/00

[Inventor]

[Residence or Address] c/o Matsushita Electric Industrial Co., Ltd, 1006, Oaza Kadoma, Kadoma-shi, Osaka

[Name] Akio Kojima

[Inventor]

[Residence or Address] c/o Matsushita Electric Industrial Co., Ltd, 1006, Oaza Kadoma, Kadoma-shi, Osaka

[Name] Yasuhiro Kuwahara

[Inventor]

[Residence or Address] c/o Matsushita Electric Industrial Co., Ltd, 1006, Oaza Kadoma, Kadoma-shi, Osaka

[Name] Tatsumi Watanabe

[Applicant]

[ID Number] 000005821

[Name] Matsushita Electric Industrial Co., Ltd.

[Agent]

[ID Number] 100097445

[Patent Attorney]

[Name] Fumio Iwasaki

[Elected Agent]

[ID Number] 100103355

[Patent Attorney]

[Name] Tomoyasu Sakaguchi

[Elected Agent]

[ID Number] 100109667

[Patent Attorney]

[Name] Hiroki Naitoh

[Expression of Fee]

[Deposit Account No.] 011305

[Amount of payment] 21,000 yen

[List of Attached Articles]

[Document Name]	Specification	1
[Document Name]	Drawings	1
[Document Name]	Abstract	1

[Number of General Power of Attorney] 9809938

[Proof request] No

[Name of The Document] Specification

[Title of The Invention]

Data Monitoring Method and Data Monitoring Apparatus

[Claims]

1. A data-monitoring method comprising:

target data for which an image can be formed;

copy-inhibition information comprising data for which copying is prohibited;

a data-monitoring means of monitoring the image created from said target data based on said copy-inhibition information; and

a copying means of creating a copy of said target data; and wherein

stops or does not perform the copying operation when said created image is considered to be said copy-inhibition information.

2. The data-monitoring method of claim 1 further comprising:

an update means of updating the copy-inhibition information of data for which copying is prohibited; and wherein

can change the copy-inhibition data.

3. The data-monitoring method of claim 2 further comprising:

an acquiring means of acquiring update information having management information for change authorization; and wherein

can change the copy-inhibition information according to the contents of the update information.

4. The data-monitoring method of claim 3 wherein said update information is provided using memory media.

5. The data-monitoring method of claim 3 wherein said update information is provided using a medium for providing information that can be checked and verified.

6. The data-monitoring method of claim 5 wherein said update information is provided over a network.

7. The data-monitoring method of claim 2 further comprising:

an automatic-information-acquisition means that searches the copy-inhibition information at a specified time as another information source; and

a log-saving means of saving a log of the update information; and wherein

when the information from the other information source differs from the saved copy-inhibition information, the method updates the copy-inhibition information.

8. The data-monitoring method of claim 1 wherein:

said first data-monitoring method further comprises

a cancellation means of stopping the function of said data-monitoring means; and

is capable of canceling the function of stopping the copying operation after the verification check.

9. A data-monitoring method comprising:

an input means of inputting an image;

a data-monitoring means of monitoring said image; and

a search means of searching for and acquiring copy-inhibition information from another information source; and wherein

it stops or does not perform input of said image when said image is found to be said copy-inhibition information.

10. The data-monitoring method of claim 7 wherein said data-monitoring method searches and acquires copy-inhibition information that is stored in a specified apparatus on a network.

11. A data-monitoring apparatus comprising:

target data for which an image can be formed;

copy-inhibition information comprising data for which copying is prohibited;

a data-monitoring means of monitoring the image created from said target data based on said copy-inhibition information; and

a copying means of creating a copy of said target data; and wherein

is such that it stops or does not perform the copying operation when said created image is considered to be said copy-inhibition information.

12. The data-monitoring apparatus of claim 11 further comprising:

an update means of updating the copy-inhibition information of data for which copying is prohibited; and wherein

is such that it can change the copy-inhibition data.

13. The data-monitoring apparatus of claim 12 further comprising:

an acquiring means of acquiring update information having management information for change authorization; and wherein

is such that it is capable of changing the copy-inhibition information according to the contents of the update information.

14. The data-monitoring apparatus of claim 13 wherein said update information is provided using memory media.

15. The data-monitoring apparatus of claim 13 wherein said update information is provided using a medium for providing information that can be checked and verified.

16. The data-monitoring apparatus of claim 15 wherein said update information is provided over a network.

17. The data-monitoring apparatus of claim 12 further comprising:

an automatic-information-acquisition means that searches the copy-inhibition information at a specified time as another information source; and

a log-saving means of saving a log of the update information; and wherein

when the information from the other information source differs from the saved copy-inhibition information, the apparatus updates the copy-inhibition information.

18. The data-monitoring apparatus of claim 11 wherein:

said first data-monitoring apparatus further comprises

a cancellation means of stopping the function of said data-monitoring means; and

is capable of canceling the function of stopping the copying operation after the verification check.

19. A data-monitoring apparatus comprising:

an input means of inputting an image;

a data-monitoring means of monitoring said image; and

a search means of searching for and acquiring copy-inhibition information from another information source; and wherein

it stops or does not perform input of said image when said image is found to be said copy-inhibition information.

20. The data-monitoring apparatus of claim 17 wherein said data-monitoring apparatus searches and acquires copy-inhibition information that is stored in a specified apparatus on a network.

[Detailed Description of the Invention]

[Field of the Invention]

[0001]

This invention relates to a data-monitoring method and data-monitoring apparatus that prevents illegal copying of confidential documents, confidential data, or copyrighted materials such as confidential data, documents, videos, printed material, paper money, stocks and bonds and all kinds of cash certificates for which copying is prohibited.

[0002]

[Description of the Related Art]

In recent years, with the advancement of networking and digitization, personal devices are being connected to networks in order to more easily obtain and print electronic data. However, as a result of DTP technology that is being developed with the objective of creating images that are true to the original document, it is possible to obtain more accurate copied materials. This is creating an environment in which is easy to obtain electronic data and to perform more accurate copying.

[0003]

On the other hand, when documents that are to be handled confidentially are copied, problems occur such as in secrecy leaks. Moreover, if it were possible to easily obtain copies that cannot be distinguished from the original document, there is a possibility that there would be more illegal use of copyrighted materials, and that copies would be used for counterfeiting of paper money and stocks and bonds, making damage large.

[0004]

Conventionally, color copiers have been equipped with an anti-counterfeiting function to prevent counterfeiting paper money or the like. Fig. 13 is a block diagram of this kind of conventional color copier. In Fig. 13, counterfeiting is prevented by a specific-image-judgment circuit 120 that uses features of an image to determine whether the image signal that is read from the scanner 110 is an image signal for paper money or a

stock or bond for which copying is prohibited, and then activates a copy-protection function that reproduces the image after performing a conversion process such as image compression or reflected image inversion, and performs a process to make it possible to easily recognize that the copied material is a copy before outputting the copy to the printer 130 (for example, the image processing apparatus disclosed in Japanese patent No. H1-316783).

[0005]

[Problems to Be Solved By the Invention]

One remarkable recent trend is not only the spread of paper copies, but also the spread of digitized documents. There is a problem, in that with the use of a personal computer, it is easy to obtain confidential electronic documents and copyrighted data over a network, and to perform a large quantity of illegal copying using a high-speed printer.

[0006]

However, this prior technology judges the image of the document read by the scanner, but does not deal with the problem related to electronic data that are read from the scanner.

[0007]

The object of this invention is to solve the aforementioned problem by providing a data monitoring method that avoids and quickly prevents illegal copying of copying-prohibited electronic data.

[Means for Solving the Problems]

[0008]

In order to save the problem described above, a first data-monitoring method of the present invention, comprises: target data for which an image can be formed; copy-inhibition information comprising data for which copying is prohibited; a data-monitoring means of monitoring the image created from the target data based on the copy-inhibition information; and a copying means of creating a copy of the target data; and is such that it stops or does not perform the copying operation when the created image is considered to be copy-inhibition information.

[0009]

A second data-monitoring method of this invention further comprises: an update means of updating the copy-inhibition information of data for which copying is prohibited, and is such that it can change the copy-inhibition data.

[0010]

A third data-monitoring method of this invention is the second data-monitoring method that further comprises an acquiring means of acquiring update information having management information for change authorization; and is such that it is capable of changing the copy-inhibition information according to the contents of the update information.

[0011]

The third data-monitoring method of this invention is such that the update information is provided using memory media.

[0012]

Also, the third data-monitoring method of this invention is such that the update information is provided using a medium for providing information that can be checked and verified.

[0013]

Moreover, the third data-monitoring method of this invention is such that the update information is provided over a network.

[0014]

Also, a fourth data-monitoring method of the invention in which the second data-monitoring method further comprises: an automatic-information-acquisition means that searches the copy-inhibition information at a specified time as another information source; and a log-saving means of saving a log of the update information; and when the information from the other information source differs from the saved copy-inhibition information, it updates the copy-inhibition information.

[0015]

A fifth data-monitoring method of the invention in which the first data-monitoring method further comprises a cancellation means of stopping the function of the data-monitoring means; and is capable of canceling the function of stopping the copying operation after the verification check.

[0016]

Moreover, a sixth data-monitoring method of the invention comprising: an input means of inputting an image; a data-monitoring means of monitoring that image; and a search means of searching for and acquiring copy-inhibition information from another information source; and is such that it stops or doe not perform input of the image when the image is found to be the copy-inhibition information.

[0017]

Also, in the fourth data-monitoring method of the invention, the data-monitoring method searches and acquires copy-inhibition information that is stored in a specified apparatus on a network.

[0018]

[Description of the Preferred Embodiments]

The preferred embodiments of the invention will be explained with reference to the drawings.

[0019]

(First Embodiment)

First, Fig. 1, Fig. 2, Fig. 3 and Fig. 4 will be used to explain a first embodiment of the invention, which is an example of a copying apparatus that prohibits illegal copying by a personal computer. Fig. 2 shows the operating environment of the personal computer. The personal computer 1 (hereafter referred to as PC 1) is installed with application software, and when configured with a simple printing system, it performs editing, processing and image processing (color processing). A scanner 3 is used for inputting images to the PC 1. A printer 2 creates a printed image

according to printing data from the PC 1 on normal paper or OHP paper. By connecting the PC 1 to a network 100, it is possible to obtain images from a network scanner 5 (hereafter referred to as NS 5) over the network 100, and to transfer printing data to a network printer 4 (hereafter referred to as NP 4) to print the data.

[0020]

A DTP system can also constructed with a PC1 that performs color processing and other processing, and a printer 2 that performs printing. Furthermore, a scanner 3 for reading images can is connected.

[0021]

Next, Fig. 1 will be used to explain the operation when the PC 1 prints specific printing data.

[0022]

Fig. 1 is a block diagram of a personal computer 1. The PC 1 specifies printing after the application software installed in the PC 1 sets the printing image, and creates printing data 11. The PC 1 also transfers the printing data 11 to the printer driver 12. The printer driver 12 is pre-installed in the PC 1 as a control program for transferring data to the printer 2. The printer driver 12 transfers the printing data 11 that are specified for printing by the application software to the printer 2.

[0023]

A printing-information-analyzing circuit 15, used as the data-monitoring means, constantly monitors the printing data 11 that are

transferred to the printer 2, and creates a final image in the confirmation memory 16 using the target data, or in other words, character-string information that is given using page notation language, image-pattern information, code information, and encryption information that is embedded using electronic-watermarking technology, and compares and analyzes it with copy-inhibition information 14. In the case that the printing information for the printing data 11 is determined to have been pre-registered in the printing-prohibited information 14, the printing-information-analyzing circuit 15 outputs a stop instruction 151 to the printer driver 12 to stop transferring printing data. The printer driver 12 stops transferring printing data according to the stop instruction 151. In this way, it is possible to prevent illegal printing on the PC 1 level. The contents of the copy-inhibition information 14 can be constantly updated according to contents for which printing is to be prohibited. In this way, it is possible to keep the contents quickly updated such that they correspond with the daily changing secrecy management level, confidential information, and anti-counterfeiting technology and encryption technology whose development is always progressing.

[0024]

This update method will be explained. When an IC card 200 is inserted, an information-update circuit 13, which functions as the update means and acquisition means, verifies the IC card 200, and only when it is determined that there is authorization to perform an update, will the update data saved on the IC card 200 be obtained. Next, the information-update circuit 13 updates the contents of the copy-inhibition information 14 based on the obtained update data. It is also possible to

obtain the update data via a network 100. By having this update function, it is possible to easily update the printing-prohibited information, and to daily update the contents with the most recent information. Since it is not necessary to replace the internal memory of the apparatus, updating can be performed quickly and it is possible to prevent the spread of illegal copying from increasing.

[0025]

Also, by performing a verification check, it is possible to prevent someone from changing the information and performing illegal printing. Moreover, it is possible to have management levels, and to manage confidential information on various levels.

[0026]

Next, Fig. 3 will be used to explain the information contained in the copy-inhibition information 14. Fig. 3 shows the information contained in the copy-inhibition information 14.

[0027]

Information that is capable of specifying a document such as character information 141 for the document data, image-pattern information 142, code information, and encryption information 144 that is embedded in the image using electronic watermarking technology is saved as copy-inhibition information.

[0028]

The title of the document and special character strings used in the

document (for example, major keywords used in a confidential document) are saved in the character information 141 for the document data. Unique pattern information that is capable of specifying the printing information is saved in the image-pattern information 142. When a document-management code is given to the original document data, analysis information for the corresponding code is saved in the code information 143. Decoding information for decoding the electronic watermark embedded in the photo-image data protected by a copyright, an decoding algorithm for decoding the encryption patter that is printed according to a pre-specified encryption (such as security printing, etc.) on the original document that is read by the scanner 3, and code-type information are saved in the encryption information. The copy-inhibition information 14 can be any information that can specify the printing information for all kinds of printed materials such as paper money, stocks and bonds, money certificates, and the like.

[0029]

Next, Fig. 4 will be used to explain the operation of the printing-information-analysis circuit 15. Fig. 4 is a block diagram of the printing-information-analysis circuit 15. The printing-information-analysis circuit 15 constantly monitors the printer driver 12 and always performs a specified operation when printing starts. First, when the operation starts, a drawing engine 154 obtains the drawing information of the printing data 11 from the printer driver 12, and performs the drawing operation according to the drawing information in the confirmation memory 16. The contents of the drawn drawing-image data 161 are analyzed by various analyzing engines. The title-analyzing

engine 155 specifies the title region in the drawing-image data 161 and transfers the analysis results of those contents to the collating circuit 159. The collating circuit 159 selects character information 141 from the copy-inhibition information 14 that can be used as collating information, and compares it with the analysis results that were transferred by the title-analyzing engine 155. When the comparison results show that there is matching information, the printing is regarded as printing of an illegal copy, and the collating circuit 159 stops the printing operation of the printer driver by signal 151.

[0030]

Similarly, the document-analyzing engine 156 detects and analyses the text region, the image-analyzing engine 157 detects and analyzes the photo region, and the code-analyzing engine 158 detects and analyzes the code region. The analysis results from each engine are transferred to the collating circuit 159. The collating circuit 159 selects character information 141, image-pattern information 142, code information 143 and encryption information 144 from the copy-inhibition information and compares that information with the analysis results that are transferred from each of the analyzing engines. When any of the results shown that there are matches, the printing is regarded as printing of an illegal copy, and the collating circuit 159 stops the printing operation of the printer driver by the signal 151. Also, the code-analyzing engine 158 could be such that it requests the necessary decoding algorithm for decoding from the collating circuit 159 and obtains the latest decoding algorithm. In this way, it is possible to always keep current with the latest encryption technology. The collating circuit 159 obtains the necessary information

from the copy-inhibition information 14 according to requests from the analyzing engines and sends that information to the respective analyzing engines.

[0031]

By having a plurality of analyzing engines in this way, it is possible to correspond to printed documents having various different document characteristics.

[0032]

With the first embodiment described above, by having a function that analyses the printing contents sent from the PC 1 to the printer when printing and prevents illegal copying, and thus it is possible to prevent illegal printing of in-house confidential documents, and prevent counterfeiting of paper money and the like. Furthermore, by having a method that is capable of easily updating illegal printing information, it is possible to quickly correspond to daily changing secrecy management levels, confidential information, and the latest progress in the development of new anti-counterfeiting technology and encryption technology. As a result, it is possible to prevent an increase in the spread of illegal printing.

[0033]

Also, by performing a verification check, it is possible to prevent someone from changing information and performing illegal printing. Moreover, it is possible to have management levels, and to manage confidential information on various levels.

[0034]

Furthermore, in the case of providing the personal computer with a function to prevent illegal printing, there is no need for special hardware, and only software needs to be installed, thus it is possible to reduce costs.

[0035]

(Second Embodiment)

In the first embodiment, the case of a personal computer having a function to prevent illegal printing was explained, however, here an embodiment of a printer having a function to prevent illegal printing will be explained.

[0036]

Fig. 2 and Fig. 5 will be used to explain the operation of the printer 2. Fig. 5 is a block diagram of the printer 2.

[0037]

The printer 2 receives the printing data from the PC 1 in the receiving buffer 21 and sends the printing data in order to the command-analyzing circuit 22. The command-analyzing circuit 22 analyzes the language of the received printing data and format of the image data. Next, when according the to the analysis results it is necessary to draw characters or graphics, the command-analyzing circuit 22 transfers the printing data to the graphics/character-drawing circuit 23. The graphics/character-drawing circuit 23 performs a specified drawing operation in the image memory 26 via the memory controller 25.

Similarly, when according to the analysis results it is necessary to create photo data, the command-analyzing circuit 22 transfers the printing data to the image-drawing circuit 27. The image-drawing circuit 27 creates the specified photo data in the image memory 26 via the memory controller 25. After the desired image data has been created in the image memory 26, the memory controller 25 transfers the image data to the printer engine 24. The printer engine 24 then prints the received image data on paper.

[0038]

The data-monitoring means comprises a printing-information-analyzing circuit 28 and copy-inhibition information 29. The printing-information-analyzing circuit 28 monitors the image data that are created in the image memory, and analyzes the contents of the image data before the image data are transferred to the printer engine 24. When the contents of the image data match the information stored in the copy-inhibition information 29, the printing-information-analyzing circuit 28 sends a signal 281 and stops the operation of the printer engine 24.

[0039]

Next, the update circuit 30, which functions as the update means, will be explained. The contents of the copy-inhibition information 29 can be constantly updated to correspond with the contents for which printing is to be prohibited. By doing so, it is possible to quickly correspond with the daily changing secrecy management level, confidential information, and constantly progressing development of anti-counterfeiting technology and encryption technology. This update method will be explained. When an

IC cared 200 is inserted, the update circuit 30 checks and verifies the IC card 200. Only after it has been determined that updating is authorized will the update circuit obtain the update data that are saved on the IC card 200. Next, based on the obtained update data, the update circuit 30 updates the contents of the copy-inhibition information 29. Also, the update data can be obtained from the PC 1. Update date can be sent together with printing data from the PC 1, regularly, irregularly, or when printing, and received by the command-analyzing circuit 22 via the receiving buffer 21. The command-analyzing circuit 22 judges the update data by an instruction code that is defined separately from the printing data, and sends the update data to the update circuit 30 by a signal 221. Based on the update data, the update circuit 30 updates the information saved in the copy-inhibition information 29. It is also possible to obtain update data from a network 100 via the PC 1.

[0040]

With this update function, it is possible to easily update the copy-inhibition information, and always keep the contents updated daily with the most recent information. Since there is no need to replaces the internal memory of the apparatus, updating can be performed quickly and it is possible to prevent an increase in the spread of illegal printing. Also, by performing a verification check, it is possible to prevent someone from changing the information and performing illegal printing. Moreover, it is also possible to have a management level function and to manage confidential information on various levels.

[0041]

Next, Fig. 6 will be used to explain the copy-inhibition information 29. Fig. 6 is a drawing showing the information that is contained in the copy-inhibition information 29. Information that can specify a document, such as character information 291 for document data, image-pattern information 292, code information 293 and encryption information 294 that is embedded in an image using electronic watermarking technology, are saved as copy-inhibition information 29.

[0042]

The title of the document and special character strings used in the document (for example, major keywords used in a confidential document) are saved in the character information 291 for the document data. Unique pattern information that is capable of specifying the printing information is saved in the image-pattern information 292. When a document-management code is given to the original document data, analysis information for the corresponding code is saved in the code information 293. Decoding information for decoding the electronic watermark embedded in the photo-image data protected by a copyright, an decoding algorithm for decoding the encryption patter that is printed according to a pre-specified encryption (such as security printing, etc.) on the original document that is read by the scanner 3, and code-type information are saved in the encryption information. The copy-inhibition information 29 can be any information that can specify the printing information for all kinds of printed materials such as paper money, stocks and bonds, money certificates, and the like.

[0043]

By simply adding the necessary information, this copy-inhibition information 29 can be made to correspond with all original copies and documents. When applying the data-monitoring method of this invention to a display system, video image information can be added, and it is possible to prevent displaying video images that are not desired. The display function is defined as a software printing function. Therefore, when seen from the user's point of view, this display function is handled the same as the printing function when interpreted as being an information-acquisition means.

[0044]

Next, Fig. 7 will be used to explain the operation of the printing-information-analyzing circuit 28. Fig. 7 is a block diagram of the printing-information-analyzing circuit 28. The printing-information-analyzing circuit 28 constantly monitors the image data 261 that are created in the image memory and always performs a specified operation when image data 261 are created. First, when the operation starts, various analyzing engines are used to analyze the contents of the image memory 26. The title-analyzing engine 285 specifies the title region in the image data 261 and transfers the analysis results of those contents to the collating circuit 289. The collating circuit 289 selects character information 291 from the copy-inhibition information 29 that can be used as collating information, and compares it with the analysis results that were transferred by the title-analyzing engine 285. When the comparison results show that there is matching information, the printing is regarded as illegal printing, and the collating circuit 289 stops the printing operation of the printer engine 24 by signal 281.

[0045]

Similarly, the document-analyzing engine 286 detects and analyses the text region, the image-analyzing engine 287 detects and analyzes the photo region, and the code-analyzing engine 288 detects and analyzes the code region. The analysis results from each engine are transferred to the collating circuit 289. The collating circuit 289 selects character information 291, image-pattern information 292, code information 293 and encryption information 294 from the copy-inhibition information and compares that information with the analysis results that are transferred from each of the analyzing engines. When any of the results show that there are matches, the printing is regarded as illegal, and the collating circuit 289 stops the printing operation of the printer engine 24 by the signal 281. Also, the code-analyzing engine 288 could be such that it requests the necessary decoding algorithm for decoding from the collating circuit 289 and obtains the latest decoding algorithm. In this way, it is possible to always keep current with the latest encryption technology. The collating circuit 289 obtains the necessary information from the copy-inhibition information 29 according to requests from the analyzing engines and sends that information to the respective analyzing engines.

[0046]

By having a plurality of analyzing engines in this way, it is possible to correspond to printed documents having various different document characteristics. Also, in the case of video-image data, the still-image engine can be applied to each image frame as the target. Moreover, by adding a video-analyzing engine (not shown in the figures) that includes

motion, it is possible to apply the engine to all kinds of video images.

[0047]

With the second embodiment described above, by having a function that analyses the printing contents when printing inside the printer 2, it is possible to prevent illegal printing of in-house confidential documents, and prevent counterfeiting of paper money and the like. Furthermore, by having a method that is capable of easily updating copy-inhibition information, it is possible to quickly correspond to daily changes in secrecy management levels, confidential information, and the latest progress in the development of new anti-counterfeiting technology and encryption technology. As a result, it is possible to prevent an increase in the spread of illegal copying.

[0048]

Also, by performing a verification check, it is possible to prevent someone from changing information and performing illegal printing. Moreover, it is possible to have management levels, and to manage confidential information on various levels.

[0049]

Furthermore, in the case of providing the printer with a function to prevent illegal printing, there is no need for a special drawing engine and other hardware, and only printer-controller software needs to be installed, thus it is possible to reduce costs.

[0050]

(Third Embodiment)

In the second embodiment, the use of a data-monitoring function in the printer for preventing illegal copying was explained, however, in this embodiment, the use of a data-monitoring function in a scanner will be explained.

[0051]

Fig. 8 will be used to explain the operation of a network scanner 5. Fig. 8 is a block diagram of a network scanner 5.

[0052]

The target document (not shown in the figure) is read by an image sensor 51 and converted to digital image data by an A/D converter 52. Here, an image-processing circuit 53 performs image processing such as specified MFT conversion and color processing, and then the image data is transferred via the network interface 54 (hereafter referred to as network I/F 54). Based on information saved in the copy-inhibition information 56, the input-information-analyzing circuit 55, which functions at the data-monitoring means, determines whether or not printing of the original document is prohibited. When it is determined that printing of the document is prohibited, the input-information-analyzing circuit 55 sends a signal 551 and stops the transfer of image data to the network I/F 54.

[0053]

The copy-inhibition information 56 is the same as the copy-inhibition information 14 shown in Fig. 3. Also, the information-update circuit 57 updates the copy-inhibition information 56. It is also possible to acquire

update information from other devices connected to network via the network I/F 54. Moreover, it is also possible to acquire update information from a removable memory card 500. When the memory card 500 is inserted, the information-update circuit 57 compares the information on the memory card 500 with the copy-inhibition information 56 and determines whether or not to update the copy-inhibition information 56.

[0054]

Also, contents that are the same as the copy-inhibition information 56 can be obtained over the network by a registration-information-search circuit 58. By doing so, there is no need to install memory for storing large amounts of information, and thus it is possible to reduce the cost of the product. Furthermore, it is also possible for the input-information-analyzing circuit 55 to automatically specify a specific database when reading the document, and obtain collation data that are the same as the copy-inhibition information 56. By doing so, there is no need for the user to update the information every time, and response is very quick. This automatic update can also be applied to the printer or personal computer.

[0055]

Even in the case of a scanner connected to the PC 1, it is possible to use the same data-monitoring function of the invention.

[0056]

With the third embodiment described above, the

registration-information-search circuit 58 of the network scanner 5 obtains contents that are the same as the copy-inhibition information 56 so there is no need to install memory for storing large amounts of information. As a result, it is possible to reduce the cost of the product.

[0057]

Moreover, by having an automatic-update function, the input-information-analyzing circuit 55 automatically specifies a specific database when reading the document and obtains collating data that are the same as the copy-inhibition information 56, so there is no need for the user to update the information every time. As a result, it is possible to always keep current with daily changes in the secrecy management level, confidential information and advances in anti-counterfeiting technology and encryption technology.

[0058]

(Fourth Embodiment)

In the third embodiment, the use of a data-monitoring function in the scanner was explained, however, in this embodiment, having a data-monitoring function in a network printer will be explained.

[0059]

Fig. 9 will be used to explain the operation of a network printer 4. Fig. 9 is a block diagram of a network printer 4.

[0060]

The network printer 4 receives printing data from an apparatus that

is connected to the network. A command-analyzing circuit 42 receives the printing data and instruction commands by way of the network interface 41 (hereafter referred to as the network I/F 41). The command analyzing circuit 42 analyzes the language and image-data format of the received printing data. Next, when according to the analysis results it is necessary to perform draw characters or graphic, the command-analyzing circuit 42 transfers the printing data to the graphics/character-drawing circuit 43. The graphics/character-drawing circuit 43 performs the specified drawing operation in the image memory 46 via the memory controller 45. Similarly, when according to the analysis results it is necessary to create photo data, the command-analyzing circuit transfers the printing data to the image-drawing circuit 47. The image-drawing circuit 47 creates the specified photo data in the image memory 46 via the memory controller 45. After the desired image data have been created in the image memory 46, the memory controller 45 transfers that image data to the printer engine 44. The printer engine 44 prints the received image data on paper.

[0061]

The data-monitoring function is constructed with the printing-information-analyzing circuit 48 and copy-inhibition information 49. The printing-information-analyzing circuit 48 monitors the printing data that were read by the command-analyzing circuit 42, and analyzes the contents of the image data before the printing data are transferred to the printer engine 44 from the image memory 46. In the case that the contents of the image data match the information saved in the copy-inhibition information 49, the printing-information-analyzing circuit 48 sends the signal 481 and

stops the operation of the printer engine 44. Similar to the second embodiment, the printing-information-analyzing circuit 48 can also monitor and analyze the image memory 46.

[0062]

Next, the update circuit 31 will be explained. It is possible to update the contents of the copy-inhibition information 49 with content that are not to be printed. This makes it possible quickly correspond to daily changes in the secrecy management level, confidential data, and advances in counterfeiting technology and encryption technology. Moreover, it is also possible for the update circuit 31 to update information saved in the copy-inhibition information 49 based on update data obtained over the network 100.

[0063]

With this fourth embodiment, the network printer 4 updates the information saved in the copy-inhibition information 49 based on update data obtained over the network 100 so it is possible to quickly prevent illegal copying.

[0064]

(Fifth Embodiment)

In the first thru the fourth embodiments, an apparatus comprising a data-monitoring function was explained, however, in this embodiment a method of quickly distributing copy-inhibition information to an apparatus having a data-monitoring function will be explained.

[0065]

Fig. 10 and Fig. 11 will be used to explain the registration function for registering the information not to be printed. Fig. 10 is a drawing explaining the registration function for apparatuses connected to the network, and Fig. 11 is a block diagram of a copy-inhibition-information-registration apparatus 6.

[0066]

In order to prevent illegal copying, it is important to detect the material to be copied as quickly as possible and determine whether to prevent copying. The copy-inhibition-information-registration apparatus 6 shown in Fig. 10 is an apparatus that distributes the copy-inhibition information over the network to the network scanner 5, network printer 4, personal computer 1 and No. n network printer 7 that are connected to the network 100. The function for preventing illegal printing in each apparatus obtains update data from the copy-inhibition-information-registration apparatus 6 by its respective update means, and updates the contents of the copy-inhibition information with the latest information. This does not place a burden on the user, and makes is possible to quickly transmit information for preventing illegal printing to each apparatus and to prevent illegal copying before it occurs.

[0067]

Next, Fig. 11 will be used to explain the copy-inhibition-information-registration apparatus 6 in detail. Fig. 11 is a block diagram of the copy-inhibition-information-registration apparatus 6.

[0068]

In Fig. 11, an information-setting means 66 acquires the copy-inhibition information from a recording medium 150.

[0069]

The recording medium can be a FD (floppy disk), MO, CD-R or any kind of medium on the copy-inhibition information can be recorded. Also, input from a keyboard, reading an image pattern using a scanner or the like can be used as other methods of acquiring information. After new information is input, the information-setting means 66 updates the printing-inhibition-registration information 65. Another method of updating the printing-inhibition-registration information 65 is a method via a network 61. In this case, a database is specified in advance in the registration-information-auto-update means 64 and set to obtain update data. The update log is saved as update-log information 63. By saving the log information, it is possible for the registration-information-auto-update means 64 to determine whether or not it is necessary to update the printing-inhibition-registration information 65 from the log information 63. The update period can be a specified time interval, or can be instructed from a pre-set database. An information-disclosure/distribution means 62 discloses the printing-inhibition-registration information 65 in response to a request via the network 100. Also, the information-disclosure/distribution means 62 distributes the printing-inhibition-registration information 65 or update information to a managed printer, scanner or personal computer.

[0070]

The case of a network printer 3 as the apparatus of the embodiment will be explained. In the network printer 4, when the copy-inhibition-information-registration apparatus 6 distributes the printing-inhibition-registration information 65, the update circuit 31 acquires the update information and rewrites the copy-inhibition information 49.

[0071]

Moreover, in the network printer 4 there is a registration-information-search circuit 33, and from an instruction from the printing-information-analyzing circuit 48, it is possible to acquire the printing-inhibition-registration information 65 directly from the information-disclosure/distribution means 62.

[0072]

By doing so, the apparatus does not need a memory for saving the copy-inhibition information 49, and thus it is possible to reduce costs. Also, by updating the printing-inhibition-registration information 65, the network printer 4 is also updated and management becomes easier and quicker to perform.

[0073]

The update record is saved as update-log information 32. By saving the log information, it is possible for the registration-information-search circuit 33 to prevent invalid searches.

[0074]

With the fifth embodiment described above, it is possible to disclose and distribute the printing-inhibition-registration information 65 from the copy-inhibition-registration apparatus to each of the apparatuses connected to the network, so management and maintenance of the apparatuses becomes easy to perform, and it is easy to make changes in the secrecy-management level.

[0075]

Also, a single change in the information, it is possible to update all of the apparatuses managed over the network, so it is possible to quickly prevent illegal copying.

[0076]

(Sixth Embodiment)

Fig. 12 will be used to explain an embodiment of a method of canceling the function for preventing illegal copying, in the case of an apparatus having a data-monitoring function. Fig. 12 is a drawing explaining a prevention-cancellation-setting circuit 16 as the means for clearing the function.

[0077]

There are times such as maintenance to the apparatus or other condition when it is necessary to cancel the function for preventing illegal printing. A user having the authority to cancel the function inserts an IC card into the prevention-cancellation-setting circuit 16 that is capable of sending a cancellation instruction. The prevention-cancellation-setting

circuit 16 checks and verifies the IC card, and instructs the printing-information-analyzing circuit 15 to stop the function. This makes it possible to stop the function for preventing illegal copying.

[0078]

Also, instead of the IC card, a cancellation method of entering a password or an encryption key over the network 100 is possible. Any method is possible in which the user can specify the authorization to cancel the function. In the prevention-cancellation-setting circuit 16 there is a function for registering the user ID, and it can be set from the network 100. This makes it possible to quickly correspond to various management states such as changes in organization, movement of the apparatus, changes in secrecy level, etc.

[0079]

With the sixth embodiment described above, the prevention-cancellation-setting circuit 16 can be used when performing maintenance of the apparatus. Also, the prevention-cancellation-setting circuit 16 has a function for registering the user ID, so management can be performed freely. This makes it possible to quickly correspond to various management states such as changes in organization, movement of the apparatus, changes in secrecy level, etc.

[0080]

With the first thru sixth embodiments it is possible to quickly prevent illegal copying.

[0081]

The data-monitoring method of this invention can be realized with CPU or DSP software. It can also be realized with hardware.

[0082]

Furthermore, since the invention can corresponds to various kinds of data, such as image data, document-text data, encryption data or the like on a scanner, printer or personal computer, it is not limited to just printing, but can also be applied to a monitor display.

[0083]

Of course it is also possible to include it in document-exchange software or document-distribution software such as database software, distribution-system software or electronic-mail software as the confidential-document-management software.

[0084]

Also, the invention is not limited to still images, but can be applied in the same way to video images, making it possible to manage video data.

[0085]

[Effect of the Invention]

As described above, with this invention, it is possible to avoid or quickly prevent illegal copying of documents or electronic data for wish copying is prohibited.

[Brief Explanation of the Drawings]

Fig. 1 is a block diagram of the personal computer 1 of a first embodiment of the invention.

Fig. 2 is a schematic drawing of the operating environment of the personal computer of the first embodiment of the invention.

Fig. 3 is a drawing showing the information that is stored in the copy-inhibition information of the first embodiment of the invention.

Fig. 4 is a block diagram of the printing-information-analyzing circuit 15 of the first embodiment of the invention.

Fig. 5 is a block diagram of the printer 2 of a second embodiment of the invention.

Fig. 6 is a drawing showing the information that is stored in the copy-inhibition information 29 of the second embodiment of the invention.

Fig. 7 is a block diagram of the printing-information-analyzing circuit 28 of the second embodiment of the invention.

Fig. 8 is a block diagram of the network scanner 5 of a third embodiment of the invention.

Fig. 9 is a block diagram of the network printer 4 of a fourth embodiment of the invention.

Fig. 10 is a drawing explaining the registration function for apparatuses connected to the network in a fifth embodiment of the invention.

Fig. 11 is a block diagram of the copy-inhibition-information-registration apparatus 6 of the fifth embodiment of the invention.

Fig. 12 is a drawing explaining the prevention-cancellation function 16 of a sixth embodiment of the invention.

Fig. 13 is a block diagram of a prior color-copy machine.

[Reference Codes]

1 Personal computer

2 Printer

3 Scanner

4 Network printer

5 Network scanner

6 Copy-inhibition-information-registration apparatus

7 No. N network printer

11 Printing data

12 Printer driver

13 Information-analyzing circuit

14 Copy-inhibition information

15 Printing-information-analyzing circuit

16 Confirmation memory

17 Prevention-cancellation-setting circuit

21 Receiving buffer

22 Command-analyzing circuit

23 Graphics/character-drawing circuit

24 Printer engine

25 Memory controller

26 Image memory

27 Image-drawing circuit

28 Printing-information-analyzing circuit

29 Copy-inhibition information

30 Update circuit

31 Update circuit

32 Update-log information

33 Registration-information-search circuit

41 Network interface

42 Command-analyzing circuit

43 Graphics/character-drawing circuit

44 Printer engine

45 Memory controller

46 Image memory

47 Image-drawing circuit

48 Printing-information-analyzing circuit

49 Copy-inhibition information

51 Image sensor

52 A/D converter

53 Image-processing circuit

54 Network interface

55 Input-information-analyzing circuit

56 Copy-inhibition information

57 Information-analyzing circuit

58 Registration-information-search circuit

61 Network interface

62 Information-disclosure/distribution means

63 Update-log information

64 Registration-information-auto-update means

65 Copy-inhibition-registration information

66 Information-setting means

100 Network

150 Recording medium

200 IC card

500 Memory card

Fig. 1

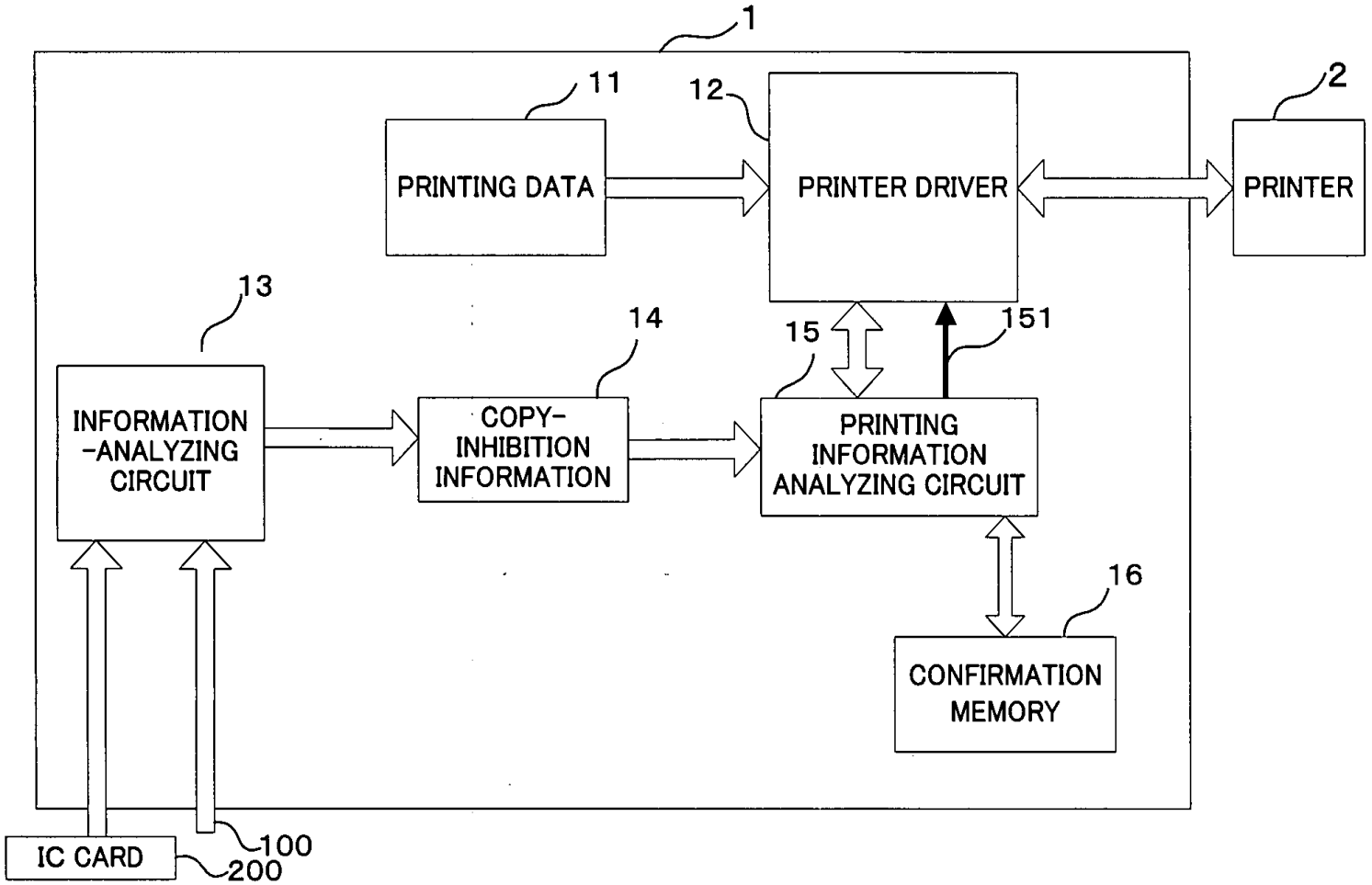

1
11
12
2
PRINTING DATA
PRINTER DRIVER
PRINTER
13
14
15
151
INFORMATION -ANALYZING CIRCUIT
COPY-INHIBITION INFORMATION
PRINTING INFORMATION ANALYZING CIRCUIT
16
CONFIRMATION MEMORY
IC CARD
100
200

Fig. 2

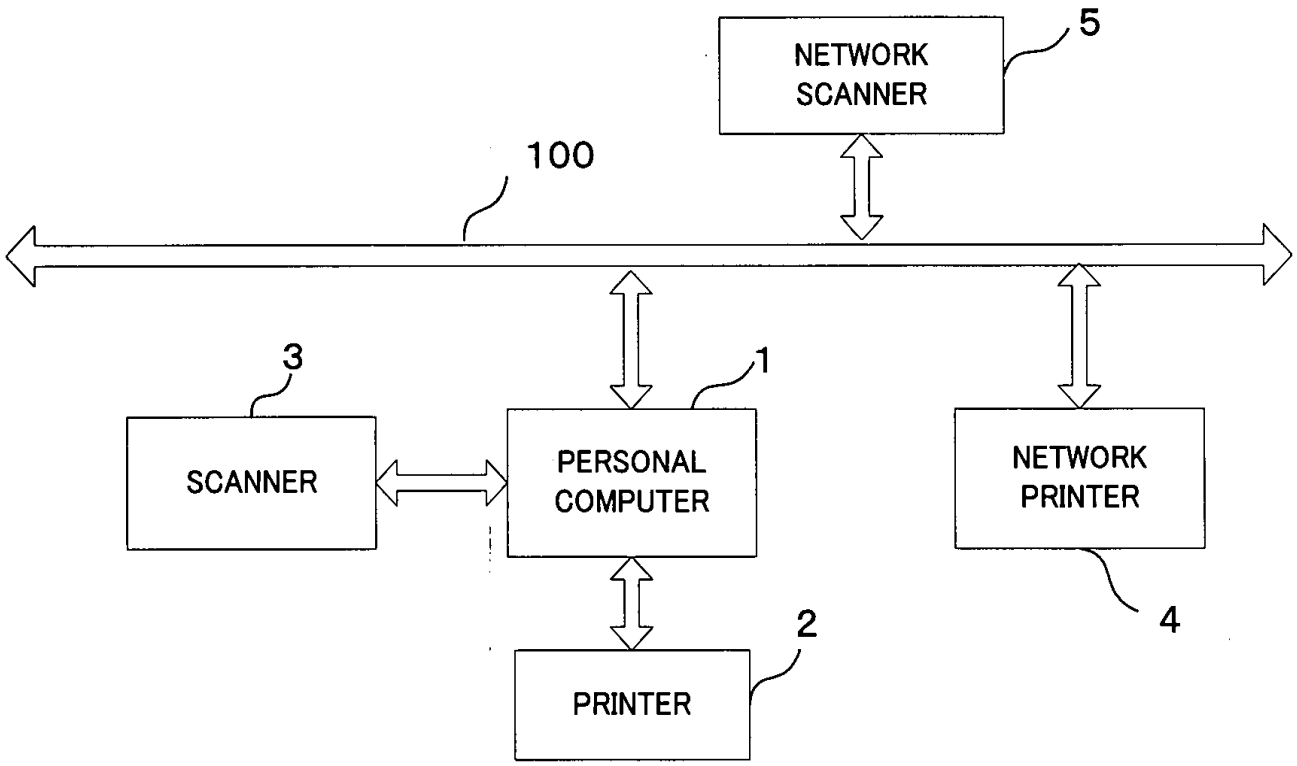

NETWORK SCANNER
5
100
3
1
SCANNER
PERSONAL COMPUTER
NETWORK PRINTER
4
2
PRINTER

Fig. 3

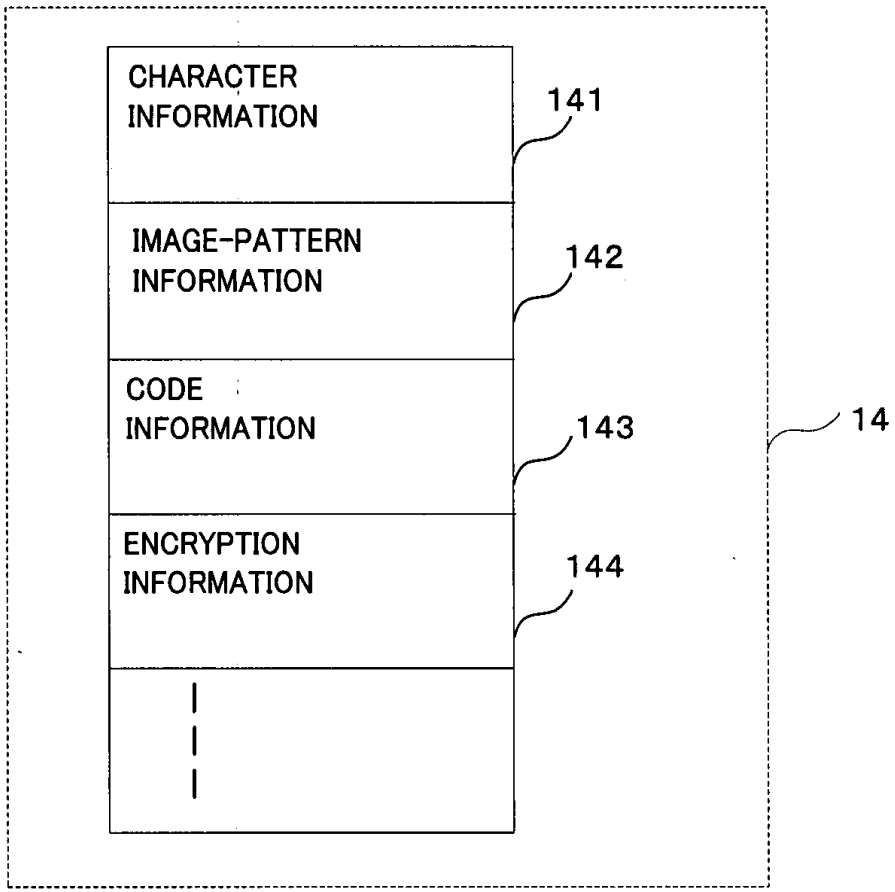

CHARACTER INFORMATION
141
IMAGE-PATTERN INFORMATION
142
CODE INFORMATION
143
ENCRYPTION INFORMATION
144
14

Fig. 4

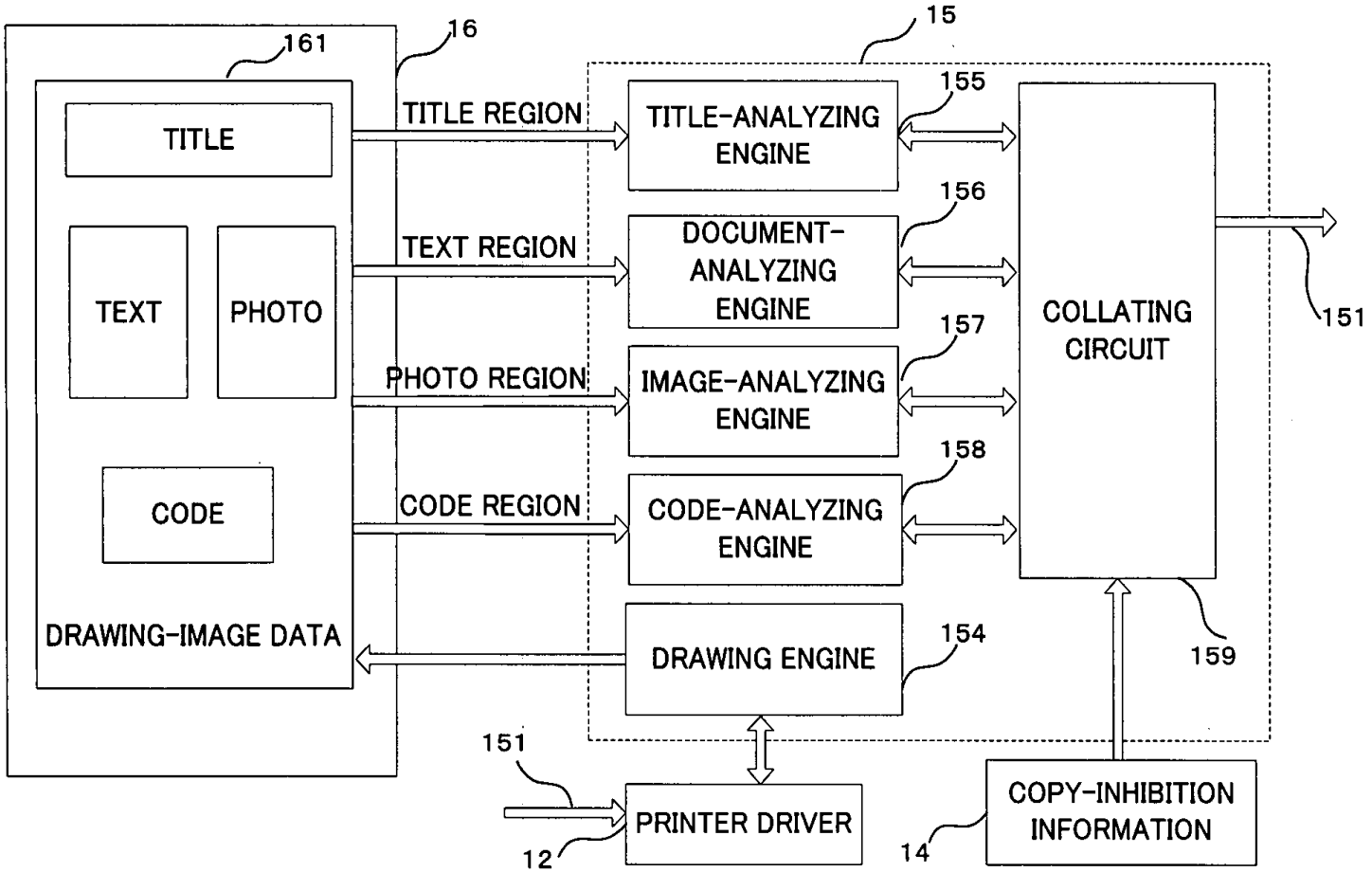

161
16
15
TITLE
TEXT
PHOTO
CODE
DRAWING-IMAGE DATA
TITLE REGION
TEXT REGION
PHOTO REGION
CODE REGION
TITLE-ANALYZING ENGINE
155
DOCUMENT-ANALYZING ENGINE
156
IMAGE-ANALYZING ENGINE
157
CODE-ANALYZING ENGINE
158
DRAWING ENGINE
154
COLLATING CIRCUIT
151
159
151
PRINTER DRIVER
12
COPY-INHIBITION INFORMATION
14

Fig. 5

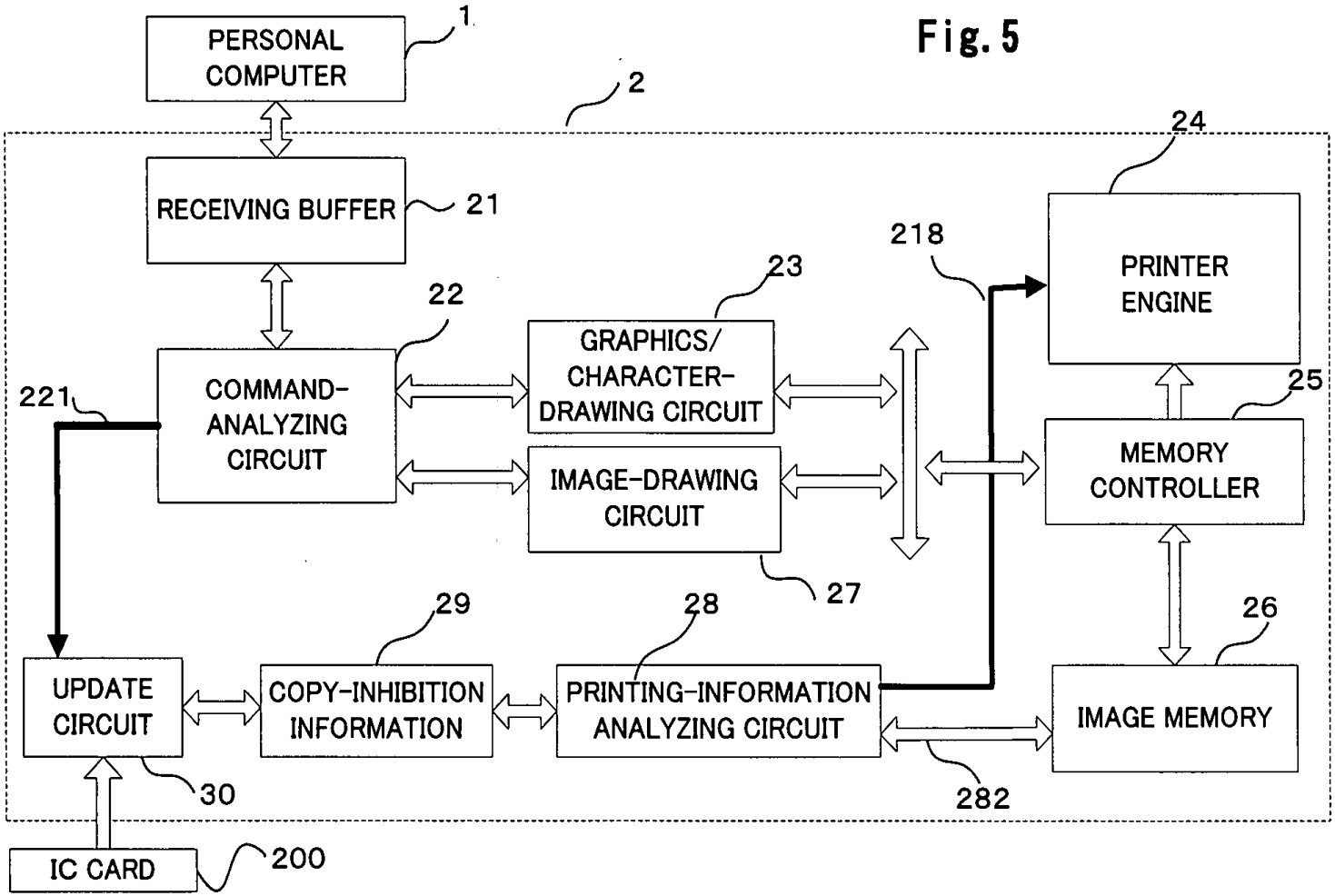

PERSONAL COMPUTER
1
2
RECEIVING BUFFER
21
22
23
24
218
PRINTER ENGINE
221
COMMAND-ANALYZING CIRCUIT
GRAPHICS/CHARACTER-DRAWING CIRCUIT
IMAGE-DRAWING CIRCUIT
27
25
MEMORY CONTROLLER
29
28
26
UPDATE CIRCUIT
COPY-INHIBITION INFORMATION
PRINTING-INFORMATION ANALYZING CIRCUIT
IMAGE MEMORY
30
282
IC CARD
200

Fig. 6

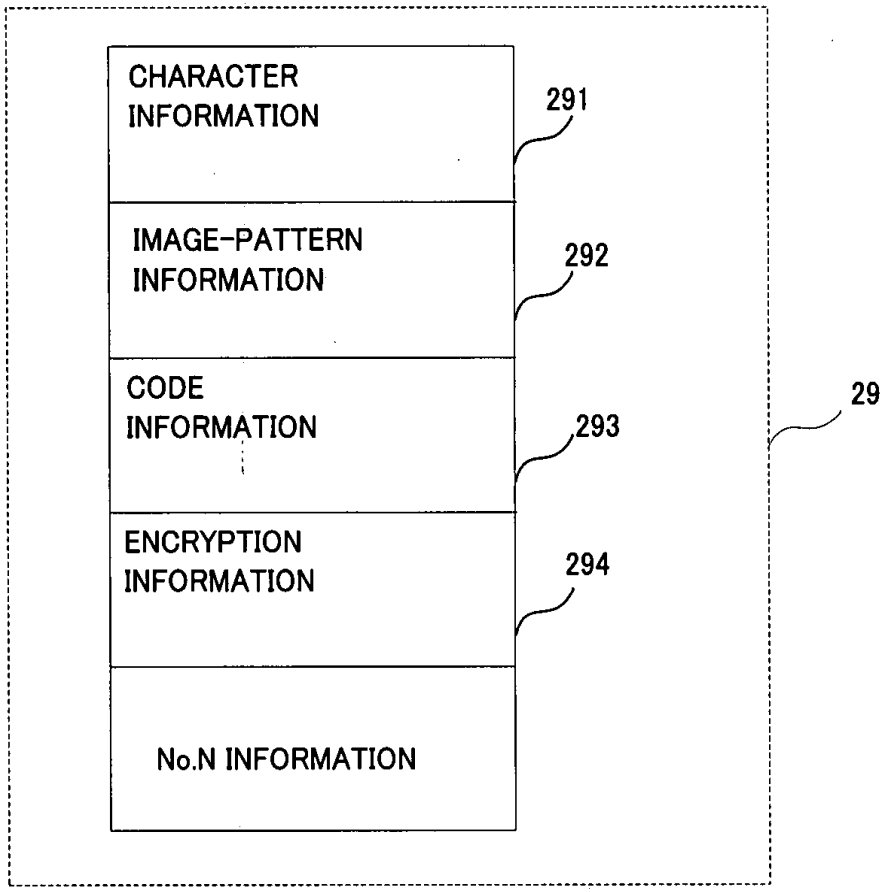

CHARACTER INFORMATION
291
IMAGE-PATTERN INFORMATION
292
CODE INFORMATION
293
ENCRYPTION INFORMATION
294
No.N INFORMATION
29

Fig. 7

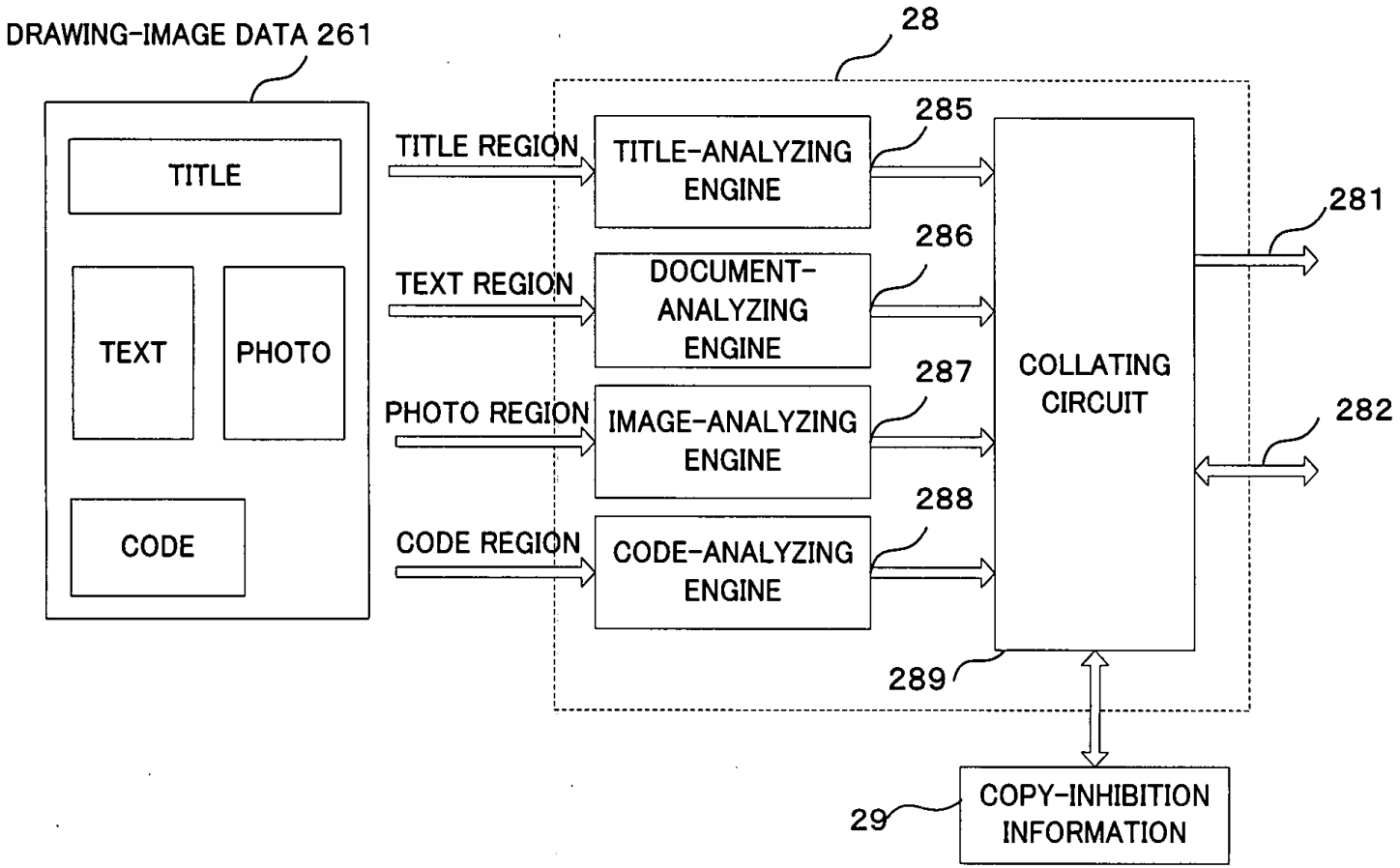

DRAWING-IMAGE DATA 261
TITLE
TEXT
PHOTO
CODE
28
TITLE REGION
TEXT REGION
PHOTO REGION
CODE REGION
TITLE-ANALYZING ENGINE
DOCUMENT-ANALYZING ENGINE
IMAGE-ANALYZING ENGINE
CODE-ANALYZING ENGINE
285
286
287
288
COLLATING CIRCUIT
281
282
289
29
COPY-INHIBITION INFORMATION

Fig. 8

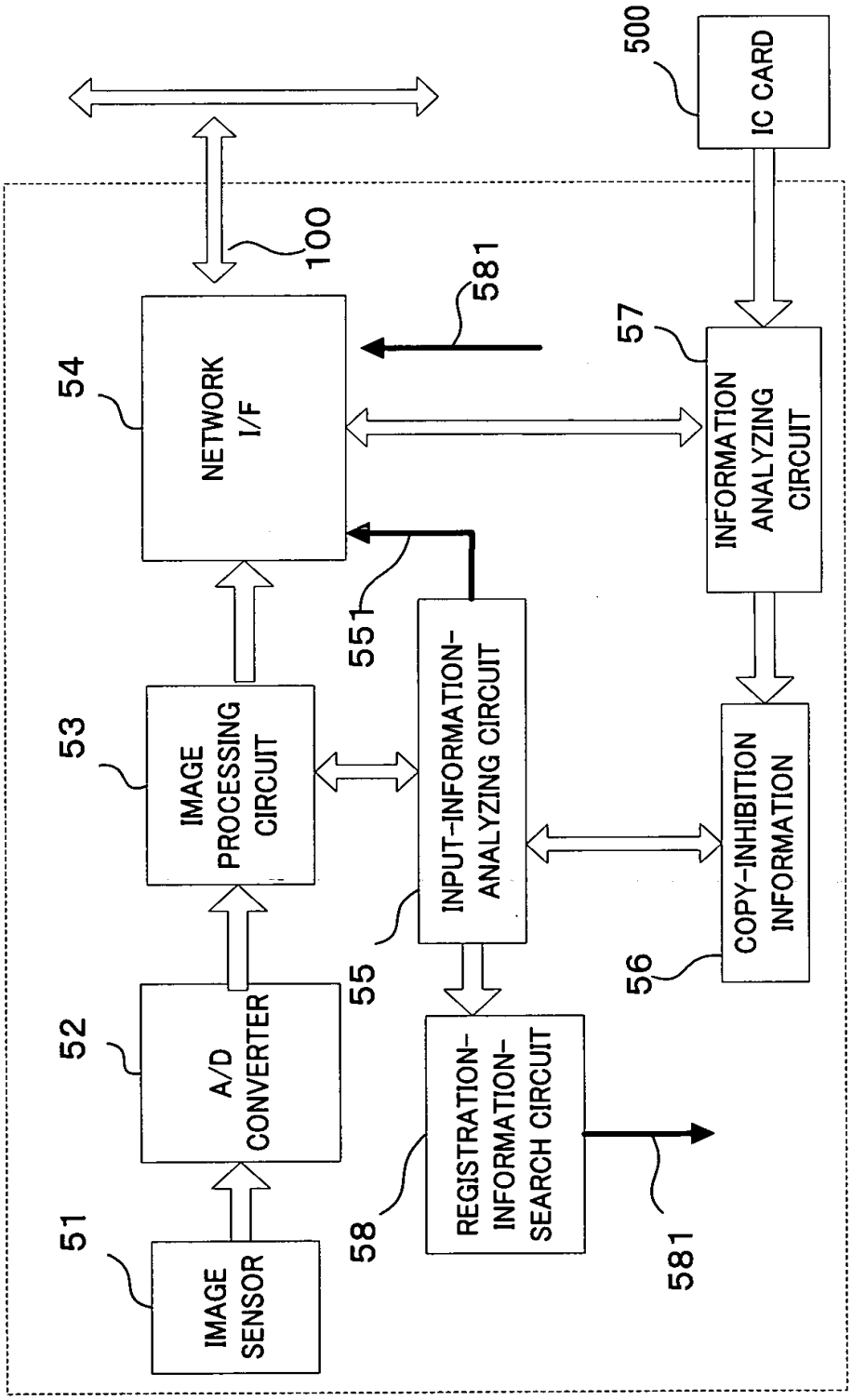

5
IMAGE SENSOR
51
A/D CONVERTER
52
IMAGE PROCESSING CIRCUIT
53
NETWORK I/F
54
100
581
551
INPUT-INFORMATION-ANALYZING CIRCUIT
55
REGISTRATION-INFORMATION-SEARCH CIRCUIT
58
581
INFORMATION ANALYZING CIRCUIT
57
COPY-INHIBITION INFORMATION
56
IC CARD
500

Fig. 9

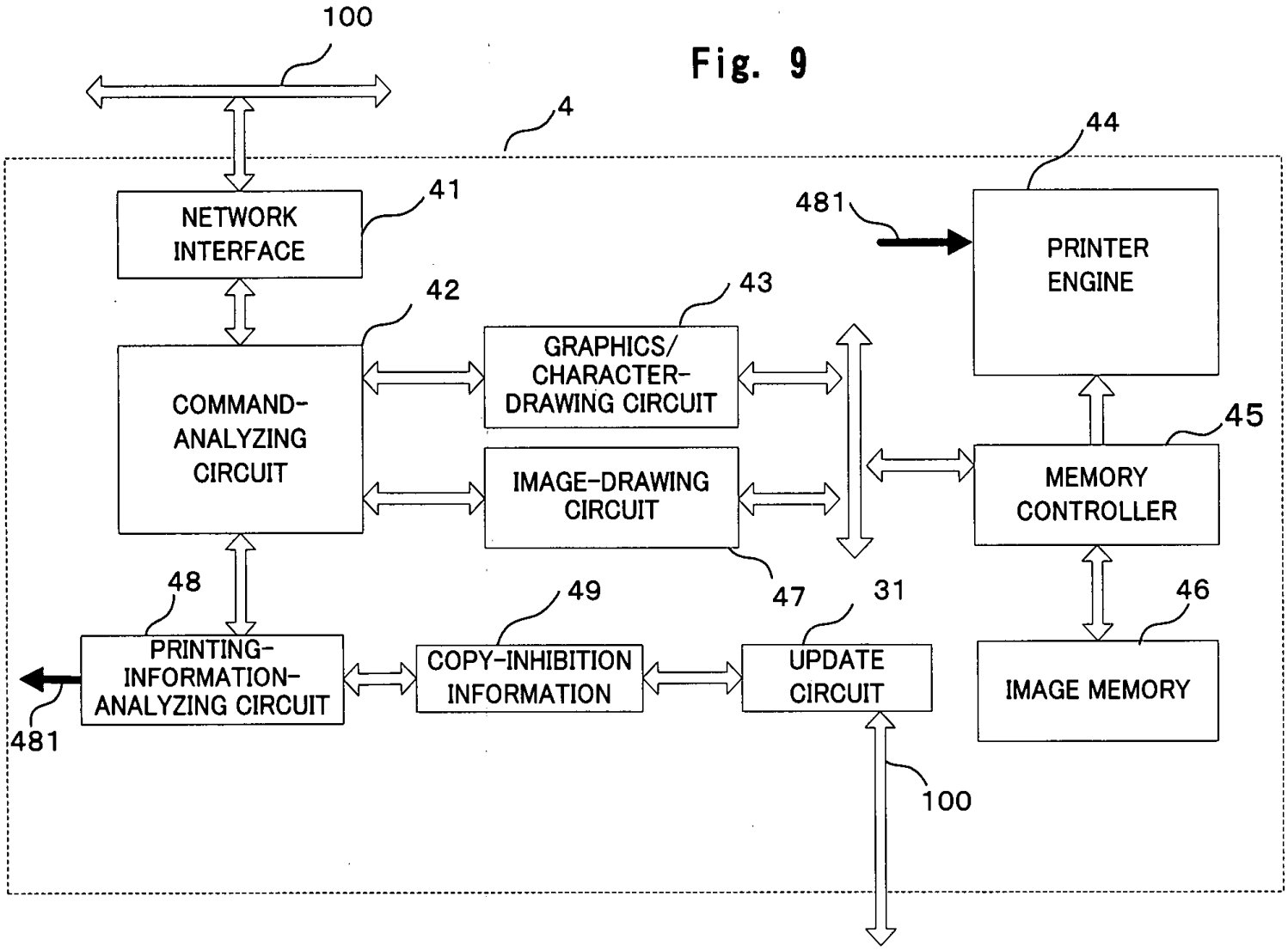

100
4
44
41
NETWORK INTERFACE
481
PRINTER ENGINE
42
43
GRAPHICS/ CHARACTER-DRAWING CIRCUIT
COMMAND-ANALYZING CIRCUIT
IMAGE-DRAWING CIRCUIT
45
MEMORY CONTROLLER
48
49
47
31
46
PRINTING-INFORMATION-ANALYZING CIRCUIT
COPY-INHIBITION INFORMATION
UPDATE CIRCUIT
IMAGE MEMORY
481
100

Fig. 10

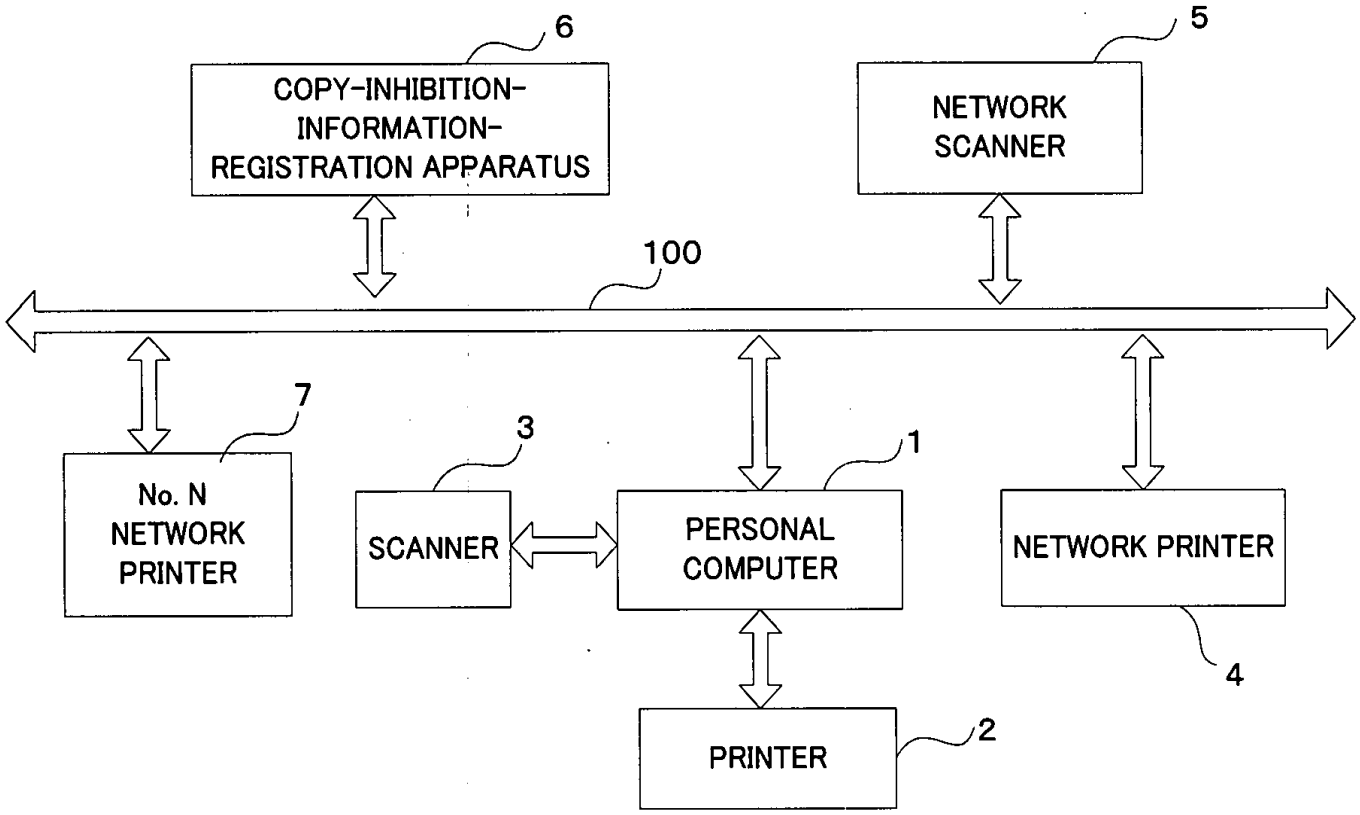

6
COPY-INHIBITION-INFORMATION-REGISTRATION APPARATUS
5
NETWORK SCANNER
100
7
No. N NETWORK PRINTER
3
SCANNER
1
PERSONAL COMPUTER
NETWORK PRINTER
4
PRINTER
2

Fig. 11

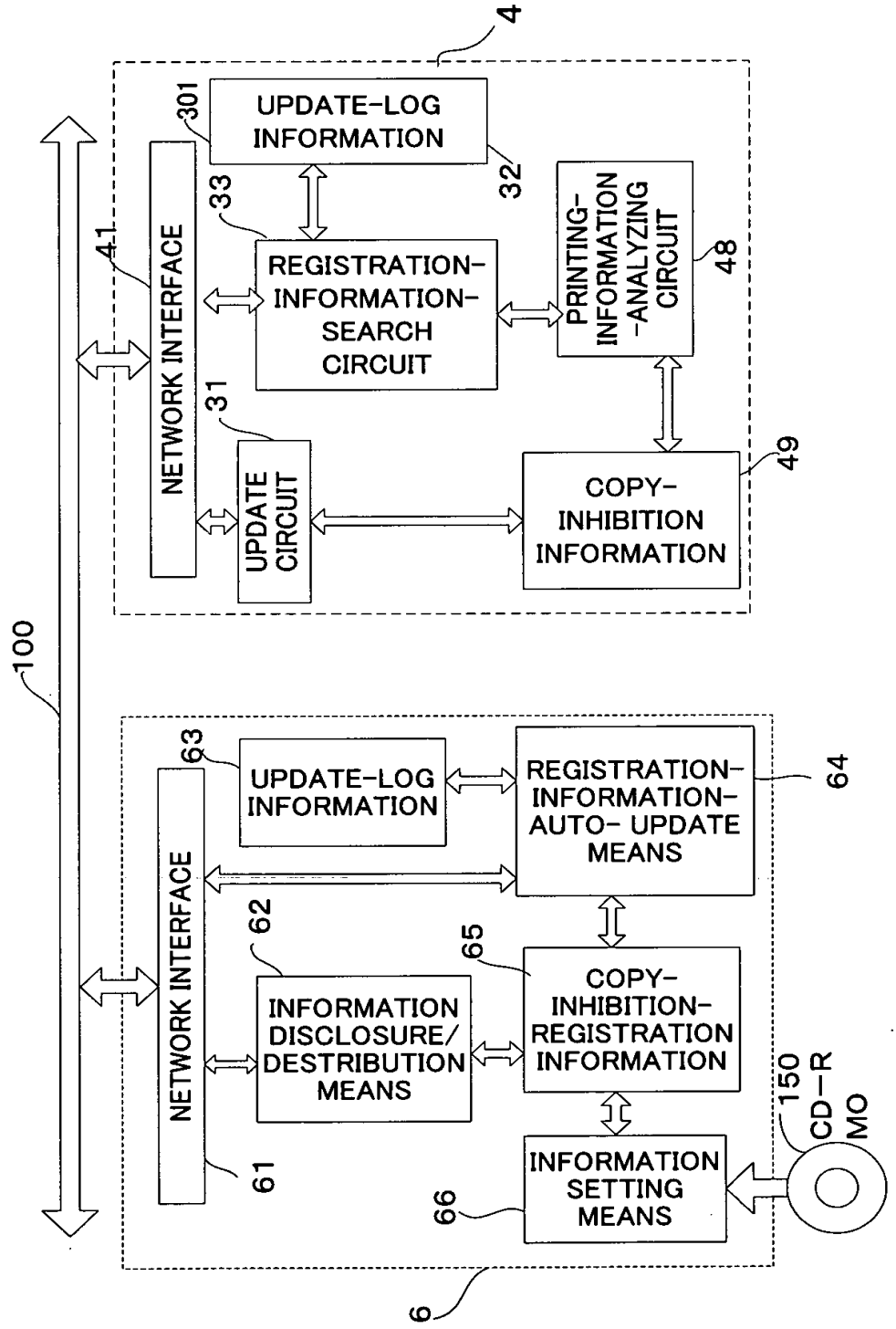

4
UPDATE-LOG INFORMATION
301
32
33
NETWORK INTERFACE
41
REGISTRATION-INFORMATION-SEARCH CIRCUIT
PRINTING-INFORMATION-ANALYZING CIRCUIT
48
31
UPDATE CIRCUIT
COPY-INHIBITION INFORMATION
49
100
63
UPDATE-LOG INFORMATION
REGISTRATION-INFORMATION-AUTO-UPDATE MEANS
64
NETWORK INTERFACE
62
65
INFORMATION DISCLOSURE/DESTRIBUTION MEANS
COPY-INHIBITION-REGISTRATION INFORMATION
150
CD-R
MO
INFORMATION SETTING MEANS
66
61
6

Fig. 12

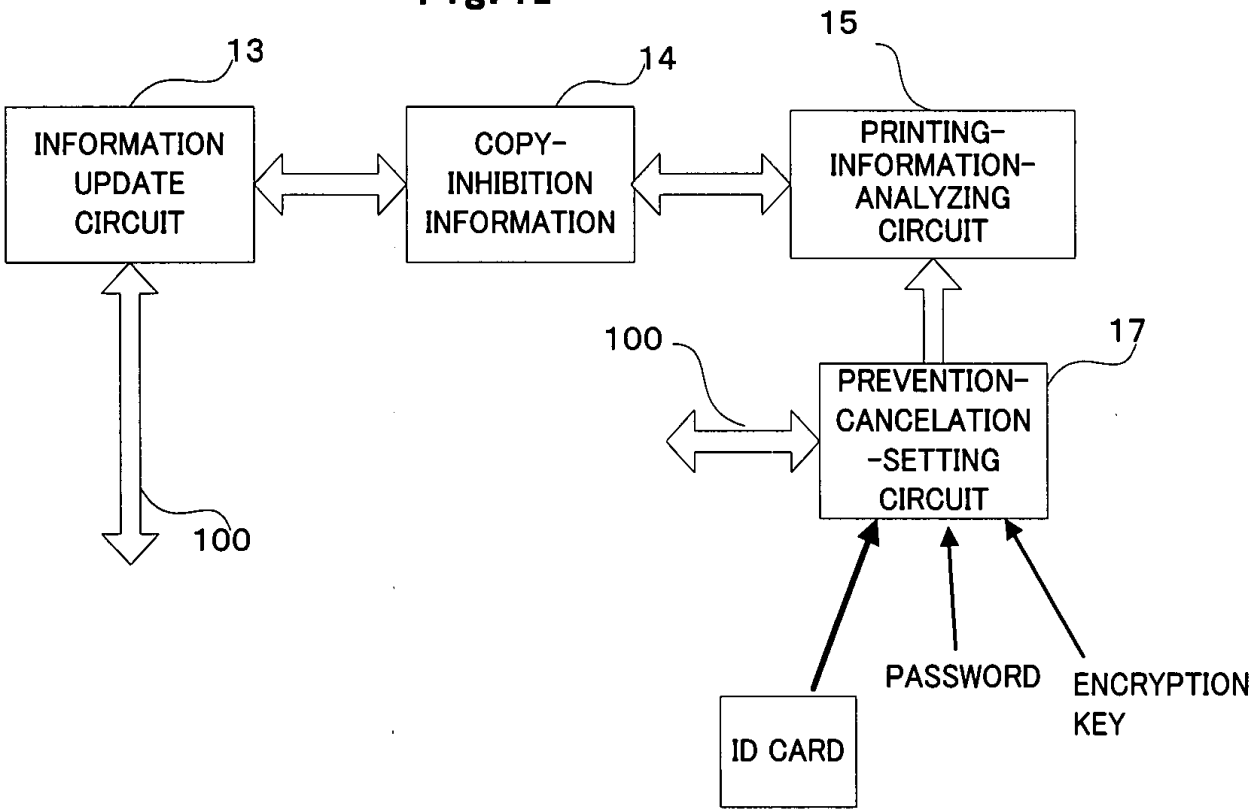
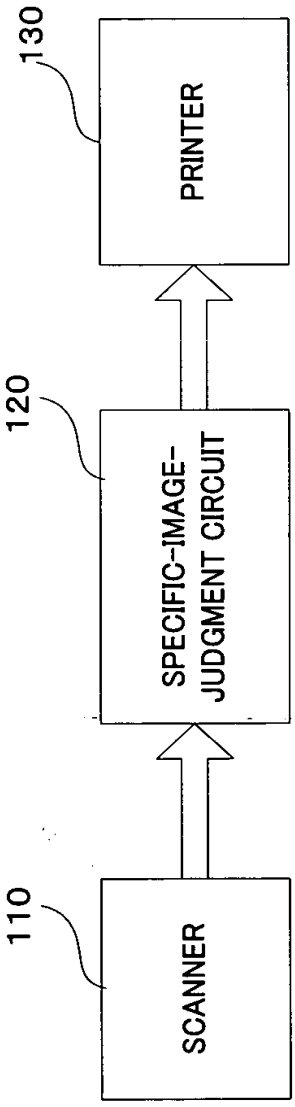

13
14
15
INFORMATION UPDATE CIRCUIT
COPY-INHIBITION INFORMATION
PRINTING-INFORMATION-ANALYZING CIRCUIT
100
17
PREVENTION-CANCELATION-SETTING CIRCUIT
100
ID CARD
PASSWORD
ENCRYPTION KEY

Fig. 13


130
PRINTER
120
SPECIFIC-IMAGE-JUDGMENT CIRCUIT
110
SCANNER

[Name of the Document] Abstract

[Summary]

[Subject]

This invention relates to a data-monitoring method that is capable of avoiding or quickly preventing illegal copying.

[Solving means]

When printing data 11 are transferred from the personal computer 1 to the printer 2 via the printer driver 12, the printing-information-analyzing circuit 15 monitors the printing data 11, and while checking the image created in the confirmation memory 16, compares and analyzes it with the information from the copy-inhibition information 14. When the image created from the printing data is determined to be registered in advance in the copy-inhibition information 14, the printing-information-analyzing circuit 15 instructs the printer driver to stop transferring printing data to the printer 2. This prevents illegal copying before the data are output to the printer 2.

[Selected Drawing] Fig. 1

09/914216
PCT/JP00/01097
06.04.00

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

JU #12/Priority Paper Mail 9/23/03

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年 ２月２６日

出願番号
Application Number: 平成１１年特許願第０４９９９７号

出願人
Applicant (s): 松下電器産業株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

２０００年 ３月 ３日

特許庁長官
Commissioner,
Patent Office 近藤隆彦

出証番号 出証特２０００－３０１２８２５

【書類名】　特許願

【整理番号】　2036610009

【提出日】　平成11年 2月26日

【あて先】　特許庁長官殿

【国際特許分類】　H04N　1/00

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　小嶋　章夫

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　▲くわ▼原　康浩

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　渡辺　辰巳

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100097445

【弁理士】

【氏名又は名称】　岩橋　文雄

【選任した代理人】

【識別番号】　100103355

【弁理士】

【氏名又は名称】　坂口　智康

【選任した代理人】

【識別番号】　100109667

【弁理士】

【氏名又は名称】　内藤　浩樹

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

【プルーフの要否】　不要

【書類名】　明細書

【発明の名称】　データ監視方法、およびデータ監視装置

【特許請求の範囲】

【請求項１】　像形成可能な対象データと、

複製が禁止されているデータ情報よりなる複製禁止情報と、

前記複製禁止情報に基づいて前記対象データから生成される展開像を監視するデータ監視手段と、

前記対象データの複製を生成する複製手段とを具備し、

前記展開像が前記複製禁止情報と見なされた時に複製動作を停止させる又は行わないことを特徴とするデータ監視方法。

【請求項２】　前記データ監視方法は、更に、

複製が禁止されているデータの複製禁止情報を更新する更新手段を具備し、

複製禁止情報の変更ができることを特徴とする請求項１記載のデータ監視方法。

【請求項３】　前記データ監視方法は、更に、

変更権限の管理情報をもつ更新情報を取得する取得手段を備し、

更新情報の内容に応じて、複製禁止情報の変更ができることを特徴とする請求項２記載のデータ監視方法。

【請求項４】　前記更新情報は、記憶メディアによって提供されることを特徴とする請求項３記載のデータ監視方法。

【請求項５】　前記更新情報は、認証確認ができる情報提供媒体によって提供されることを特徴とする請求項３記載のデータ監視方法。

【請求項６】　前記更新情報は、ネットワークによって提供されることを特徴とする請求項５記載のデータ監視方法。

【請求項７】　前記データ監視方法は、更に、

他の情報源に、所定の時間で複製禁止情報を問い合わせる情報自動取得手段と、

更新情報の履歴を保存する履歴保存手段と、を有し、

他の情報源と自ら保有する複製禁止情報とが異なるときに、複製禁止情報を更

新することを特徴とする請求項２記載のデータ監視方法。

【請求項８】　前記データ監視方法は、更に、

前記データ監視手段の機能を停止させる解除手段を具備し、

認証確認後に複製を停止させる機能を解除できることを特徴とする請求項１記載のデータ監視方法。

【請求項９】　像画像を入力する入力手段と、

前記像画像を監視するデータ監視手段と、

他の情報源に複製禁止情報を問い合わせ、情報を取得する問い合わせ手段と、を具備し、

前記像画像が前記複製禁止情報と見なされた時に前記像画像の入力を停止させる又は行わないことを特徴とするデータ監視方法。

【請求項１０】　前記データ監視方法は、ネットワーク上の所定の装置に蓄積された複製禁止情報を問い合わせ、取得することを特徴とする請求項７記載のデータ監視方法。

【請求項１１】　像形成可能な対象データと、

複製が禁止されているデータ情報よりなる複製禁止情報と、

前記複製禁止情報に基づいて前記対象データから生成される展開像を監視するデータ監視手段と、

前記対象データの複製を生成する複製手段と、

前記展開像が前記複製禁止情報と見なされた時に複製動作を停止させる又は行わないように制御する制御手段と、を具備することを特徴とするデータ監視装置。

【請求項１２】　前記データ監視装置は、更に、

複製が禁止されているデータの複製禁止情報を更新する更新手段を具備し、

複製禁止情報の変更ができることを特徴とする請求項１１記載のデータ監視装置。

【請求項１３】　前記データ監視装置は、更に、

変更権限の管理情報をもつ更新情報を取得する取得手段を備し、

更新情報の内容に応じて、複製禁止情報の変更を行うことを特徴とする請求項

１２記載のデータ監視装置。

【請求項１４】　前記更新情報は、記憶メディアによって提供されることを特徴とする請求項１３記載のデータ監視装置。

【請求項１５】　前記更新情報は、認証確認ができる情報提供媒体によって提供されることを特徴とする請求項１３記載のデータ監視装置。

【請求項１６】　前記更新情報は、ネットワークによって提供されることを特徴とする請求項１５記載のデータ監視装置。

【請求項１７】　前記データ監視装置は、更に、

他の情報源に、所定の時間で複製禁止情報を問い合わせる情報自動取得手段と、

更新情報の履歴を保存する履歴保存手段と、を有し、

他の情報源と自ら保有する複製禁止情報とが異なるときに、複製禁止情報を更新することを特徴とする請求項１２記載のデータ監視装置。

【請求項１８】　前記データ監視装置は、更に、

前記データ監視手段の機能を停止させる解除手段を具備し、

認証確認後に複製を停止させる機能を解除できることを特徴とする請求項１１記載のデータ監視装置。

【請求項１９】　像画像を入力する入力手段と、

前記像画像を監視するデータ監視手段と、

他の情報源に複製禁止情報を問い合わせ、情報を取得する問い合わせ手段と、を具備し、

前記像画像が前記複製禁止情報と見なされた時に前記像画像の入力を停止させる又は行わないことを特徴とするデータ監視装置。

【請求項２０】　前記データ監視装置は、ネットワーク上の所定の装置に蓄積された複製禁止情報を問い合わせ、取得することを特徴とする請求項１７記載のデータ監視装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、機密文書、機密データ、著作権物など複製が禁止された機密データ、文書、動画像、印刷物、紙幣や有価証券または各種金券等に対し、不正な複製を防止するデータ監視方法、及びその装置に関するものである。

【０００２】

【従来の技術】

近年、ネットワーク化、デジタル化の進展によって、個々の機器がネットワークに接続されて、電子データを手軽に取得、印刷できるようになってきた。一方、ＤＴＰでは作成原稿データに忠実な画像形成を目的として技術開発が進められた結果、高精細な複製物が得られるようになってきた。これによって、電子データを取得し、高精細な印刷が簡単にできる環境が整いつつある。

【０００３】

一方で機密管理された文書に対しては複製されると機密漏洩等問題になる。また、オリジナル原稿と区別がつかない複製物が簡単に得られると、著作物の不正使用、さらには、紙幣や有価証券など偽造に悪用される恐れがあり、被害が大きい。

【０００４】

従来より、カラー複写機には紙幣等に対し偽造防止機能が搭載されていた。図１３は従来のカラー複写機のブロック図である。図１３において、スキャナ１１０から読み込まれた画像信号は、特定画像判定回路１２０によって複写が禁止されている紙幣や証券類の画像信号かどうかを画像特徴より判別し、縮小画像、鏡像反転などの変換処理を行ってから画像を再生したりする複写防止機能を起動することにより、複写物が容易に偽造物とわかる処理をしてプリンタ１３０に出力し、偽造を防止していた（例えば、特開平１－３１６７８３の画像処理装置）。

【０００５】

【発明が解決しようとする課題】

近年の傾向として紙による原稿だけでなく、電子化された文書の普及も目さましい。パーソナルコンピュータによって、ネットワーク上から簡単に機密電子文書、著作物データを入手し、高速プリンタで大量に不正印刷できるという課題がある。

【０００６】

ところで、上記先行技術は、スキャナから読み取られた原稿の画像を判別するものであるので、スキャナから読み取られない電子データに係る上記課題には対処できない。

【０００７】

本発明は、上記課題を解決するもので、複製が禁止された電子データの不正な複製を未然に、かつ迅速に防止するデータ監視法を提供することを目的とする。

【０００８】

【課題を解決するための手段】

上記課題を解決するために、本発明における第１のデータ監視方法は、像形成可能な対象データと、複製が禁止されているデータ情報よりなる複製禁止情報と、前記複製禁止情報に基づいて前記対象データから生成される展開像を監視するデータ監視手段と、前記対象データの複製を生成する複製手段とを有し、前記展開像が前記複製禁止情報と見なされた時に複製動作を停止させる又は行わないように構成している。

【０００９】

また、本発明における第２のデータ監視方法は、第１のデータ監視方法に、更に、複製が禁止されているデータの複製禁止情報を更新する更新手段を有し、複製禁止情報の変更ができるように構成している。

【００１０】

また、本発明における第３のデータ監視方法は、第２のデータ監視方法に、更に、前記データ監視方法は、更に、変更権限の管理情報をもつ更新情報を取得する取得手段を備し、

更新情報の内容に応じて、複製禁止情報の変更ができるように構成したものである。

【００１１】

また、本発明における第３のデータ監視方法において、前記更新情報は記憶メディアによって提供されるように構成したものである。

【００１２】

また、本発明における第３のデータ監視方法において、前記更新情報は認証確認ができる情報提供媒体によって提供されるように構成したものである。

【００１３】

また、本発明における第３のデータ監視方法において、前記更新情報はネットワークによって提供されるように構成したものである。

【００１４】

また、本発明における第４のデータ監視方法は、第２のデータ監視方法に、更に、他の情報源に、所定の時間で複製禁止情報を問い合わせる情報自動取得手段と、更新情報の履歴を保存する履歴保存手段とを有し、他の情報源と自ら保有する複製禁止情報とが異なるときに、複製禁止情報を更新するように構成したものである。

【００１５】

また、本発明における第５のデータ監視方法は、第１のデータ監視方法に、更に、前記データ監視手段の機能を停止させる解除手段を具備し、認証確認後に複製を停止させる機能を解除できるように構成したものである。

【００１６】

また、本発明における第６のデータ監視方法は、像画像を入力する入力手段と、前記像画像を監視するデータ監視手段と、他の情報源に複製禁止情報を問い合わせ、情報を取得する問い合わせ手段とを具備し、前記像画像が前記複製禁止情報と見なされた時に前記像画像の入力を停止させるように構成したものである。

【００１７】

また、本発明における第４のデータ監視方法において、前記データ監視方法はネットワーク上の所定の装置に蓄積された複製禁止情報を問い合わせ、取得するように構成したものである。

【００１８】

【発明の実施の形態】

以下、本発明の実施の形態について図面を参照しながら説明する。

【００１９】

（第１の実施の形態）

まず、本発明の第１の実施の形態で、パーソナルコンピュータにおける不正な複製を禁止するデータ監視方法を組み込む一実施例を図１、図２、図３、図４を用いて説明する。　図２はパーソナルコンピュータの使用環境の構成図を示したものである。パーソナルコンピュータ１（以下、パーソナルコンピュータ１をＰＣ１と記述する。）には、様々なアプリケーション・ソフトウェアが搭載され、簡易な印刷システムを構成した場合には編集処理、加工処理、画像処理（色処理）を行う。スキャナ３は画像をＰＣ１に入力するのに使われる。複製手段としてのプリンタ２はＰＣ１の印刷データに従って用紙、ＯＨＰ用紙等に印字イメージの像形成を行う。ＰＣ１はネットワーク１００に接続されると、ネットワーク１００上のネットワークスキャナ５（以下、ＮＳ５と記述する。）から画像を取り込んだり、ネットワークプリンタ４（以下ＮＰ４と記述する。）に印刷データを転送して印刷もできる。

【００２０】

ＤＴＰシステムは、色処理、加工を行うＰＣ１、印刷するプリンタ２があれば構成できる。更に、原稿を読み取るのにスキャナ３を接続する。

【００２１】

次に、図１を用いて、ＰＣ１が特定の印刷データ１１を印刷する場合の動作を説明する。

【００２２】

図１はパーソナルコンピュータ１のブロック図である。ＰＣ１にインストールされたアプリケーションで印刷イメージが確定すると印刷指定が行われ、印刷データ１１が生成される。さらに、印刷データ１１はプリンタドライバ１２に渡される。プリンタドライバ１２は、ＰＣ１からプリンタ２にデータの橋渡しを行う制御プログラムとして、予めインストールされているものである。このプリンタドライバ１２はアプリケーションより印刷指定された印刷データ１１をプリンタ２に転送する。

【００２３】

データ監視手段としての印刷情報解析回路１５は、プリンタ２に転送される印刷データ１１を常にモニターし、対象データとしてのページ記述言語などで記載

された文字列情報、画像パターン情報、コード情報、電子透かし技術で埋め込まれた暗号情報などを確認メモリ１６の中で最終的な展開像に事前に形成し、複製禁止情報１４からの情報と照合および解析を行なう。もし、この印刷データ１１の印刷情報が予め複製禁止情報１４に登録されているものと判定した場合は、プリンタドライバ１２に対して印刷データの転送を停止させる停止命令１５１を出力する。プリンタドライバ１２は、停止命令１５１によって、印刷データの転送を停止する。これによって、不正な印刷をＰＣ１レベルで防止できる。　複製禁止情報１４の内容は、印刷を禁止したい内容に対し、常に対応して更新できるようにする。これによって、日々変更される機密管理レベル、機密情報、日新月歩で技術開発が進歩する偽造防止技術、暗号化技術に迅速に対応できる。

【００２４】

この更新方法について説明する。更新手段および取得手段としての情報更新回路１３は、ＩＣカード２００が挿入されると、ＩＣカード２００の認証を行う。更新権利があると判定した場合のみ、ＩＣカード２００に保存された更新データを取得する。次に、情報更新回路１３は、取得した更新データに基づいて、複製禁止情報１４の内容を更新する。また、更新データはネットワーク１００を経由して入手しても良い。この更新機能を持つことで、禁止印刷情報の更新が簡単に行え、日常的に更新される最新情報に内容を維持することができる。機器に内蔵したメモリ交換が不要なので、更新を迅速に行え、不正印刷の広がりの拡大を防止できる。

【００２５】

また、認証確認を行うことで、情報の改ざん、不正な印刷を行う者に対する改造防止ができる。また、管理レベルを持たせることもでき、機密情報の管理を様々な階層レベルで実現できる。

【００２６】

次に、図３を用いて、複製禁止情報１４の格納情報について説明する。図３は複製禁止情報１４の格納情報を示した図である。

【００２７】

複製禁止情報１４としては、文書データの文字情報１４１、画像パターン情報

１４２、コード情報１４３、画像中に電子透かし技術で挿入された暗号情報１４４など、文書を特定できる情報が保存されている。

【００２８】

文書データの文字列情報１４１には、文書中のタイトル、文書中の特定文字列（例えば、機密文書の主要なキーワードなど）を保存する。画像パターン情報１４２には、印刷情報を特定できる固有のパターン情報が保存される。コード情報１４３には、原稿データに文書管理コードが付与される場合に対応するコードの解析情報が保存される。暗号情報１４４には、著作権で保護された写真画像データに埋め込まれた電子透かし解読情報や、スキャナ３で読み込む原稿に予め所定の暗号化（セキュリティー印刷等）によって印刷されている暗号パターンの解読アルゴリズム、コードの種別情報などが保存される。複製禁止情報１４は、文書、紙幣、証券、金券などあらゆる印刷物を対象に、印刷情報を特定できるものであれば何でも良い。

【００２９】

次に、図４を用いて、印刷情報解析回路１５の動作を説明する。図４は印刷情報解析回路１５のブロック図である。印刷情報解析回路１５は、プリンタドライバ１２を常にモニターし、印刷を開始する際に必ず所定の動作を行うようにする。まず、動作を開始すると描画エンジン１５４は、プリンタドライバ１２から印刷データ１１の描画情報を入手し、確認メモリ１６に描画情報に従って描画動作を行う。描画された描画画像データ１６１は、各種の解析エンジンによって、内容が解析される。描画画像データ１６１の中のタイトル領域はタイトル解析エンジン１５５が領域を特定し、その内容の解析結果を照合回路１５９に転送する。照合回路１５９は複製禁止情報１４の中から、照合情報として使える文字情報１４１を選び出し、タイトル解析エンジン１５５が転送してきた解析結果と照合する。照合の結果、一致する情報が発見されると不正印刷の印字と見なし、信号１５１によってプリンタドライバ１２の印刷動作を停止させる。

【００３０】

同様に、文書解析エンジン１５６はテキスト領域を検出し内容を解析し、イメージ解析エンジン１５７は写真領域を検出し内容を解析し、コード解析エンジン

１５８はコード領域を検出し内容を解析する。解析結果は、それぞれ照合回路１５９に転送される。照合回路１５９は複製禁止情報１４の中から、照合情報として使える文字情報１４１、画像パターン情報１４２、コード情報１４３、暗号情報１４４をそれぞれ選択し、各種解析エンジンから転送されてくる解析結果と照合する。照合の結果、いずれかの一致検出が発見されると不正印刷の印字と見なし、信号１５１によってプリンタドライバ１２の印刷動作を停止させる。また、コード解析エンジン１５８は解読に必要なデコードアルゴリズムを照合回路１５９に問い合わせて最新の解読アルゴリズムを入手できるようにする。これによって、日新月歩する暗号技術に常に対応できる。照合回路１５９は、各解析エンジンからの問合わせに応じ、複製禁止情報１４の中から必要な情報を入手して各解析エンジンに返答する。

【００３１】

このように、複数の解析エンジンを有することで、文書特徴の異なる様々な印刷原稿に対応できる。

【００３２】

以上、第１の実施の形態によれば、ＰＣ１からプリンタに印刷を行う際に印刷内容を解析し、不正印刷を防止する機能を持たせることで、社内の機密文書の不正印刷、紙幣、金権の偽造などを未然に防ぐことができる。さらに、不正印刷情報を簡単に更新できる仕組みを持つことで、日々変更される機密管理レベル、機密情報、日新月歩で技術開発が進歩する偽造防止技術、暗号化技術に迅速に対応できる。結果、不正印刷の広がりの拡大を防止できる。

【００３３】

また、認証確認を行うことで、情報の改ざん、不正な印刷を行う者に対する改造防止ができる。また、管理レベルを持たせることもでき、機密情報の管理を様々な階層レベルで実現できる。

【００３４】

また、パーソナルコンピュータに不正印刷防機能を持たせる場合は、特別なハードウェアはいらなく、ソストウェアのみをインストールすれば良く、低コストで実現できる。

【００３５】

（第２の実施の形態）

第１の実施の形態ではパーソナルコンピュータに不正印刷防止機能を組み込む場合を説明したが、ここではプリンタに不正印刷防止機能を持たせる一実施例を説明する。

【００３６】

図２、図５を用いて、プリンタ２の動作を説明する。図５はプリンタ２のブロック図である。

【００３７】

プリンタ２はＰＣ１からの印刷データを受信バッファ２１で受け、コマンド解析回路２２に順次印刷データを送る。コマンド解析回路２２は受け取った印刷データの言語、画像データフォーマットを解析する。次に、コマンド解析回路２２は解析した結果により、文字、図形描画を行う必要があれば、図形／文字描画回路２３に印刷データを転送する。図形／文字描画回路２３は、メモリコントローラ２５を経由して、画像メモリ２６に所定の描画動作を行う。同様に、コマンド解析回路２２は解析した結果により、写真データを展開する必要があれば、イメージ描画回路２７に印刷データを転送する。イメージ描画回路２７は、メモリコントローラ２５を経由して、画像メモリ２６に所定の写真データを展開する。メモリコントローラ２５は画像メモリ２６に所望の画像データが形成されるとプリンタエンジン２４に画像データを転送する。プリンタエンジン２４は、受け取った画像データから紙に印刷を行う。

【００３８】

データ監視手段は、印刷情報解析回路２８と複製禁止情報２９により構成される。印刷情報解析回路２８は、画像メモリに展開される画像データをモニターし、プリンタエンジン２４に画像データが転送される前に、画像データの内容を解析する。もし、画像データの内容が、複製禁止情報２９に保存された情報と一致した場合は、信号２８１により、プリンタエンジン２４の動作を停止させる。

【００３９】

次に、更新手段としての更新回路３０について説明する。複製禁止情報２９の

内容は、印刷を禁止したい内容に対し、常に対応して更新できるようにする。これによって、日々変更される機密管理レベル、機密情報、日新月歩で技術開発が進歩する偽造防止技術、暗号化技術に迅速に対応できる。この更新方法について説明する。更新回路３０は、ＩＣカード２００が挿入されると、ＩＣカード２００の認証を行う。更新権利があると判定した場合のみ、ＩＣカード２００に保存された更新データを取得する。次に、更新回路３０は、取得した更新データに基づいて、複製禁止情報２９の内容を更新する。また、更新データはＰＣ１より入手しても良い。印刷データの他に、定期的、不定期、印刷時でも良いが、更新データを一緒にＰＣ１より送り、受信バッファ２１経由してコマンド解析回路２２が受ける。コマンド解析回路２２は印刷データと別に定義された命令コードから更新データを判定し、信号２２１を経由して更新回路３０に更新データを送付する。更新回路３０は更新データに基づき、複製禁止情報２９の保存情報を更新する。更に、ネットワーク１００よりＰＣ１を経由して更新データを入手しても良い。

【００４０】

この更新機能を持つことで、禁止印刷情報の更新が簡単に行え、日常的に更新される最新情報に内容を維持することができる。機器に内蔵したメモリ交換が不要なので、更新を迅速に行え、不正印刷の広がりの拡大を防止できる。また、認証確認を行うことで、情報の改ざん、不正な印刷を行う者に対する改造防止ができる。また、管理レベルを持たせることもでき、機密情報の管理を様々な階層レベルで実現できる。

【００４１】

次に、図６を用いて、複製禁止情報２９の説明を行う。図６は複製禁止情報２９の格納情報を示した図である。複製禁止情報２９としては、文書データの文字情報２９１、画像パターン情報２９２、コード情報２９３、画像中に電子透かし技術で挿入された暗号情報２９４など、文書を特定できる情報が保存されている。

【００４２】

文書データの文字列情報２９１には、文書中のタイトル、文書中の特定文字列

（例えば、機密文書の主要なキーワードなど）を保存する。画像パターン情報２９２には、印刷情報を特定できる固有のパターン情報が保存される。コード情報２９３には、原稿データに文書管理コードが付与される場合に対応するコードの解析情報が保存される。暗号情報２９４には、著作権で保護された写真画像データに埋め込まれた電子透かし解読情報や、スキャナ３で読み込む原稿に予め所定の暗号化（セキュリティー印刷等）によって印刷されている暗号パターンの解読アルゴリズム、コードの種別情報などが保存される。複製禁止情報２９は、文書、紙幣、証券、金券などあらゆる印刷物を対象に、印刷情報を特定できるものであれば何でも良い。

【００４３】

この複製禁止情報２９は、必要な情報を追加するだけで、あらゆる文書、原稿に対応できる。表示システムに本発明のデータ監視方法を導入する際には、動画像情報を追加すれば良く、見せたくない動画の表示も防止する事ができる。表示機能は、ソウトウェア的印刷機能を定義される。よって、ユーザーからみた場合は表示機能も情報を得る手段と解釈すれば印刷機能と同等に扱われる。

【００４４】

次に、図７を用いて、印刷情報解析回路２８の動作を説明する。図７は印刷情報解析回路２８のブロック図である。印刷情報解析回路２８は、画像メモリに展開される画像データ２６１をモニターし、画像データ２６１が形成さる際に必ず所定の動作を行うようにする。まず、動作を開始すると各種解析エンジンを用いて画像メモリ２６の内容を解析する。画像データ２６１の中のタイトル領域はタイトル解析エンジン２８５が領域を特定し、その内容の解析結果を照合回路２８９に転送する。照合回路２８９は複製禁止情報２９の中から、照合情報として使える文字情報２９１を選び出し、タイトル解析エンジン２８５が転送してきた解析結果と照合する。照合の結果、一致する情報が発見されると不正印刷の印字と見なし、信号２８１によってプリンタエンジン２４の印刷動作を停止させる。

【００４５】

同様に、文書解析エンジン２８６はテキスト領域を検出し内容を解析し、イメージ解析エンジン２８７は写真領域を検出し内容を解析し、コード解析エンジン

２８８はコード領域を検出し内容を解析する。解析結果は、それぞれ照合回路２８９に転送される。照合回路２８９は複製禁止情報２９の中から、照合情報として使える文字情報２９１、画像パターン情報２９２、コード情報２９３、暗号情報２９４をそれぞれ選択し、各種解析エンジンから転送されてくる解析結果と照合する。照合の結果、いずれかの一致検出発見されると不正印刷の印字と見なし、信号２８１によってプリンタエンジン２４の印刷動作を停止させる。また、コード解析エンジン２８８は解読に必要なデコードアルゴリズムを照合回路２８９に問い合わせて最新の解読アルゴリズムを入手できるようにする。これによって、日新月歩する暗号技術に常に対応できる。照合回路２８９は、各解析エンジンからの問合わせに応じ、複製禁止情報２９の中から必要な情報を入手して各解析エンジンに返答する。

【００４６】

このように、複数の解析エンジンを有することで、文書特徴の異なる様々な印刷原稿に対応できる。また、動画像データに対しては、フレーム画像を対象に静止画像エンジンを適用できる。また、動きを含む動画解析エンジンの追加（図示せず）によって、あらゆる動画像にも適用できる。

【００４７】

以上、第２の実施の形態によれば、プリンタ２の内部で印刷を行う際に印刷内容を解析し、不正複写を防止する機能を持たせることで、社内の機密文書の不正印刷、紙幣、金権の偽造などを未然に防ぐことができる。さらに、複製禁止情報を簡単に更新できる仕組みを持つことで、日々変更される機密管理レベル、機密情報、日新月歩で技術開発が進歩する偽造防止技術、暗号化技術に迅速に対応できる。結果、不正複写の広がりの拡大を防止できる。

【００４８】

また、認証確認を行うことで、情報の改ざん、不正な印刷を行う者に対する改造防止ができる。また、管理レベルを持たせることもでき、機密情報の管理を様々な階層レベルで実現できる。

【００４９】

また、プリンタに不正な複製を防止するデータ監視機能を持たせる場合は、特

別な描画エンジン、ハードウェアはいらなく、プリンタコントローラのソストウェアのみ変更すれば良く、低コストで実現できる。

【００５０】

（第３の実施の形態）

第２の実施の形態ではプリンタに不正な複製を防止するデータ監視機能を組み込む場合を説明したが、ここではスキャナにデータ監視機能を持たせる一実施例を説明する。

【００５１】

図８を用いて、ネットワークスキャナ５の動作を説明する。図８はネットアークスキャナ５のブロック図である。

【００５２】

対象となる原稿（図示せず）をイメージセンサ５１によって読み取り、Ａ／Ｄ変換器５２によってデジタル画像データに変換する。ここで、所定のＭＦＴ変換、カラー処理等画像処理が画像処理回路５３で行われ、ネットワークインタフェース５４（以下、ネットワークＩ／Ｆ５４と記す。）を経由して、画像データの転送が行われる。データ監視手段としての入力情報解析回路５５は複製禁止情報５６に保存された情報に基づいて印刷が禁止されている原稿かどうかの判定を行う。もし、禁止されている原稿を検出した場合は、信号５５１によってネットワークＩ／Ｆ５４に対し、画像データの転送を停止させる。

【００５３】

複製禁止情報５６は図３に図示する複製禁止情報１４と同様のものである。また、複製禁止情報５６は情報更新回路５７によって、更新される。ネットワーク上に接続された他の機器からネットワークＩ／Ｆ５４を経由して更新データを取得しても良い。さらに、着脱可能なメモリーカード５００からの更新情報から取得しても良い。メモリーカード５００の着脱の時に、「更新する」、「更新しない」を情報更新回路５７が、複製禁止情報５６と、メモリカード５００を照合し、変更の有無から判定する。

【００５４】

また、複製禁止情報５６と同様の内容は、登録情報問い合わせ回路５８によ

ってネットワークを経由して入手することもできる。これによって、膨大な情報を格納するメモリを搭載する必要がなく、製品コストを削減できる。更に、読み取りを行うと、入力情報解析回路５５が特定のデーターベースを自動的に指定し、複製禁止情報５６と同じ照合データを入手する仕組みを持つ。これによって、ユーザーが都度、更新する必要がなくなる。また、迅速な対応もできる。この自動更新は、他のプリンタ、パーソナルコンピュータにも適用できる。

【００５５】

なお、スキャナはＰＣ１に接続されるものでも、同様に本発明のデータ監視機能を組み込むことができる。

【００５６】

以上、第３の実施の形態によれば、ネットワークスキャナ５は、複製禁止情報５６と同様の内容を登録情報問い合わせ回路５８によってネットワークを経由して入手するので、膨大な情報を格納するメモリを搭載する必要がない。結果、製品コストを削減できる。

【００５７】

また、読み取りを行うと、入力情報解析回路５５が特定のデーターベースを自動的に指定し、複製禁止情報５６と同じ照合データを入手する自動更新機能の仕組みを持つので、ユーザーが都度、更新する必要がなくなる。結果、日々変更される機密管理レベル、機密情報、日新月歩で技術開発が進歩する偽造防止技術、暗号化技術に迅速に対応できる。

【００５８】

（第４の実施の形態）

第３の実施の形態ではスキャナにデータ監視機能を組み込む場合を説明したが、ここではネットワークプリンタにデータ監視機能を持たせる一実施例を説明する。

【００５９】

図９を用いて、ネットワークプリンタ４の動作を説明する。図９はネットワークプリンタ４のブロック図である。

【００６０】

ネットワークプリンタ４はネットワーク上に接続された機器から印刷データを受け取る。コマンド解析回路４２はネットワークインタフェース４１（以下、ネットワークＩ／Ｆ４１と記す。）を経由して印刷データ、命令コマンドのやりとりを行う。コマンド解析回路４２は受け取った印刷データの言語、画像データフォーマットを解析する。次に、コマンド解析回路４２は解析した結果により、文字、図形描画を行う必要があれば、図形／文字描画回路４３に印刷データを転送する。図形／文字描画回路４３は、メモリコントローラ４５を経由して、画像メモリ４６に所定の描画動作を行う。同様に、コマンド解析回路４２は解析した結果により、写真データを展開する必要があれば、イメージ描画回路４７に印刷データを転送する。イメージ描画回路４７は、メモリコントローラ４５を経由して、画像メモリ４６に所定の写真データを展開する。メモリコントローラ４５は画像メモリ４６に所望の画像データが形成されるとプリンタエンジン４４に画像データを転送する。プリンタエンジン４４は、受け取った画像データから紙に印刷を行う。

【００６１】

データ監視機能は、印刷情報解析回路４８と複製禁止情報４９により構成される。印刷情報解析回路４８は、コマンド解析回路４２で解釈される印刷データをモニターし、プリンタエンジン４４に画像メモリ４６から印刷データが転送される前に、画像データの内容を解析する。もし、画像データの内容が、複製禁止情報４９に保存された情報と一致した場合は、信号４８１により、プリンタエンジン４４の動作を停止させる。第２の実施の形態同様に、印刷情報解析回路４８は画像メモリ４６をモニターし解析しても良い。

【００６２】

次に、更新回路３１について説明する。複製禁止情報４９の内容は、印刷を禁止したい内容に合わせて更新できる。これによって、日々変更される機密管理レベル、機密情報、日新月歩で技術開発が進歩する偽造防止技術、暗号化技術に迅速に対応できる。また、更新回路３１は、ネットワーク１００より入手した更新データに基づき、複製禁止情報４９の保存情報を更新することもできる。

【００６３】

以上、第４の実施の形態によれば、ネットワークプリンタ４は、ネットワーク１００より入手した更新データに基づき、複製禁止情報４９の保存情報を更新するので、不正な複製を迅速に防止できる。

【００６４】

（第５の実施の形態）

第１から第４の実施の形態ではデータ監視機能を組み込んだ装置について説明したが、ここではデータ監視機能を組み込んだ装置に対して、複製禁止情報を迅速に配信できる方法の一実施例を説明する。

【００６５】

図１０、図１１を用いて、印刷を禁止したい情報の登録機能について説明する。図１０はネットワーク上に接続された機器への登録機能説明図である。図１１は複製禁止情報登録装置６のブロック図である。

【００６６】

不正な複製を防止するためには、いかに迅速に目的とする複製物を検出し、複製を防止するかが重要である。図１０に図示する複製禁止情報登録装置６はネットワーク１００上に接続されたネットワークスキャナ５，ネットワークプリンタ４、パーソナルコンピュータ１、第ｎのネットワークプリンタ７に対して、複製禁止情報をネットワーク経由で配信する装置である。各装置に組み込まれた不正印刷防止機能は、個々に組み込まれた更新手段によって、複製禁止情報登録装置６からの更新データを取得し、複製禁止情報の内容を最新のものに更新する。これによって、ユーザに負担をかけることなく、迅速に不正印刷の情報を各機器に伝達でき、不正な複製を未然に防止できる。

【００６７】

次に、図１１を用いて、複製禁止情報登録装置６の詳細を説明する。図１１は複製禁止情報登録装置６のブロック図である。

【００６８】

図１１において、情報設定手段６６は、記録媒体１５０により複製禁止情報を取得する。

【００６９】

記録媒体は、ＦＤ（フロッピーディスク）、ＭＯ、ＣＤ－Ｒ等複製禁止情報を記録出きるものであれば良い。また、別な情報取得方法として、キーボードからの入力、スキャナなどによる画像パターンの読み取りなどがある。情報設定手段６６は、新規な情報が入力されると、禁止印刷登録情報６５を更新する。禁止印刷登録情報６５を更新する別な方法としてネットワーク６１を経由する方法もある。この場合は、登録情報自動更新手段６４に、予め決められたデータベースを指定して更新データを入手するように設定しておく。更新記録は、更新履歴情報６３として保存する。履歴情報を保存することで、登録情報自動更新手段６４が履歴情報６３から禁止印刷登録情報６５を更新する必要が「ある」、「ない」を判定できる。更新周期は所定の時間間隔でも良いし、予め決められたデータベースからの通知によってでも良い。情報開示／配信手段６２は、ネットワーク１００を経由した問合わせに対し、禁止印刷登録情報６５を開示する。また、管理下に置かれたプリンタ、スキャナ、パーソナルコンピュータに対して禁止印刷登録情報６５の配信、または更新情報の配信を行う。

【００７０】

機器側の実施例として、ネットワークプリンタ４の場合を説明する。ネットワークプリンタ４では、禁止印刷登録情報６５の配信が複製禁止情報登録装置６より行われると、更新回路３１が更新情報を取得し、複製禁止情報４９を書き換える。

【００７１】

また、ネットワークプリンタ４には登録情報問合わせ回路３３があり、印刷情報解析回路４８の指示により情報開示／配信手段６２から直接に禁止印刷登録情報６５を取得することもできる。

【００７２】

これによって、装置側は複製禁止情報４９の保存メモリが不要になり、コストを削減できる。また、禁止印刷登録情報６５を更新すれば、ネットワークプリンタ４も更新されるので、管理がしやすく、迅速な対応ができる。

【００７３】

更新記録は、更新履歴情報３２として保存する。履歴情報を保存することで、

登録情報問合わせ回路３３は無効な問い合わせを防止できる。

【００７４】

以上、第５の実施の形態によれば、複製禁止情報登録装置６からネットワークに接続された各機器に対し禁止印刷登録情報６５を開示／配信できるので、機器管理、機器メンテナンス、機密情報レベルの変更が行いやすい。

【００７５】

また、一カ所の情報変更で、ネットワーク上の管理された機器を一斉に更新することができるので、迅速に不正な複製を防止できる。

【００７６】

（第６の実施の形態）

データ監視機能を組み込んだ装置に対して、不正な複製を防止する機能を解除する方法の一実施例を図１２を用いて説明する。図１２は、解除手段としての防止解除設定回路１６の説明図である。

【００７７】

装置のメンテナンスや、何らかの都合により、不正印刷の防止機能を解除したい場合がある。機能を解除する権限を有するユーザは解除命令を行うことができるＩＣカードを防止解除設定回路１６に挿入する。防止解除設定回路１６は、ＩＣカードの認証を行い、印刷情報解析回路１５に機能停止を指示する。これによって、不正な複製を防止する機能を停止できる。

【００７８】

また、ＩＣカードに代わり、ネットワーク１００を経由してパスワードによる解除方法や、暗号キーによる解除方法でも良い。いずれにしても、解除権限をもつユーザが特定できる方法であれば良い。防止解除設定回路１６には、ユーザ認証の登録機能をもち、ネットワーク１００から設定できる。これにより、組織の変更、機器の移動、機密レベルの変更等、様々な管理状態に迅速に対応できる。

【００７９】

以上、第６の実施の形態によれば、防止解除設定回路１６を利用することで、機器メンテナンスができる。また、防止解除設定回路１６はユーザ認証の登録機能をもつので、自在な管理を可能にする。これにより、組織の変更、機器の移動

、機密レベルの変更等、様々な管理状態に迅速に対応できる。

【００８０】

以上、第１の実施の形態から第６の実施の形態によれば、迅速に不正な複製を防止することができる。

【００８１】

なお、本発明のデータ監視方法は、ＣＰＵ、ＤＳＰによるソフトウェアによって実現できる。また、専用のハードウェアによって実現しても良い。

【００８２】

さらには、スキャナ、プリンタ、パーソナルコンピュータ上で、原稿画像データ、文書テキストデータ、暗号データなど様々な特徴のデータに対応できることから、印刷に限らず、モニター表示にも利用できる。

【００８３】

また、機密文書管理ソフトウェアとしてデーターベース、流通システム、電子メール等の文書交換ソフトウェア、ドキュメントの配信ソフトウェアに組み込むことも、もちろんできる。

【００８４】

また、静止画像にとどまらず、動画画像にも同様に適用でき、動画データ管理にも応用することができる。

【００８５】

【発明の効果】

以上のように、本発明によれば、複製が禁止された原稿、電子データ等の不正な複製を未然に、かつ迅速に防止することができる。

【図面の簡単な説明】

【図１】

本発明の第１の実施の形態であるパーソナルコンピュータ１のブロック図

【図２】

本発明の第１の実施の形態であるパーソナルコンピュータの使用環境の構成図

【図３】

本発明の第１の実施の形態である複製禁止情報１４の格納情報を示した図

【図４】

本発明の第１の実施の形態である印刷情報解析回路１５のブロック図

【図５】

本発明の第２の実施の形態であるプリンタ２のブロック図

【図６】

本発明の第２の実施の形態である複製禁止情報２９の格納情報を示した図

【図７】

本発明の第２の実施の形態である印刷情報解析回路２８のブロック図

【図８】

本発明の第３の実施の形態であるネットアークスキャナ５のブロック図

【図９】

本発明の第４の実施の形態であるネットワークプリンタ４のブロック図

【図１０】

本発明の第５の実施の形態であるネットワーク上に接続された機器への登録機能説明図

【図１１】

本発明の第５の実施の形態である複製禁止情報登録装置６のブロック図

【図１２】

本発明の第６の実施の形態である防止解除１６の説明図

【図１３】

従来のカラー複写機のブロック図

【符号の説明】

１　パーソナルコンピュータ

２　プリンタ

３　スキャナ

４　ネットワークプリンタ

５　ネットワークスキャナ

６　複製禁止情報登録装置

７　第Ｎのネットワークプリンタ

１１　印刷データ
１２　プリンタドライバ
１３　情報更新回路
１４　複製禁止情報
１５　印刷情報解析回路
１６　確認メモリ
１７　防止解除設定回路
２１　受信バッファ
２２　コマンド解析回路
２３　図形／文字描画回路
２４　プリンタエンジン
２５　メモリコントローラ
２６　画像メモリ
２７　イメージ描画回路
２８　印刷情報解析回路
２９　複製禁止情報
３０　更新回路
３１　更新回路
３２　更新履歴情報
３３　登録情報問い合わせ回路
４１　ネットワークインタフェース
４２　コマンド解析回路
４３　図形／文字描画回路
４４　プリンタエンジン
４５　メモリコントローラ
４６　画像メモリ
４７　イメージ描画回路
４８　印刷情報解析回路
４９　複製禁止情報

５１　イメージセンサ

５２　Ａ／Ｄ変換器

５３　画像処理回路

５４　ネットワークインタフェース

５５　入力情報解析回路

５６　複製禁止情報

５７　情報更新回路

５８　登録問い合わせ回路

６１　ネットワークインタフェース

６２　情報開示／配信手段

６３　更新履歴情報

６４　登録情報自動更新手段

６５　複製禁止登録情報

６６　情報設定手段

１００　ネットワーク

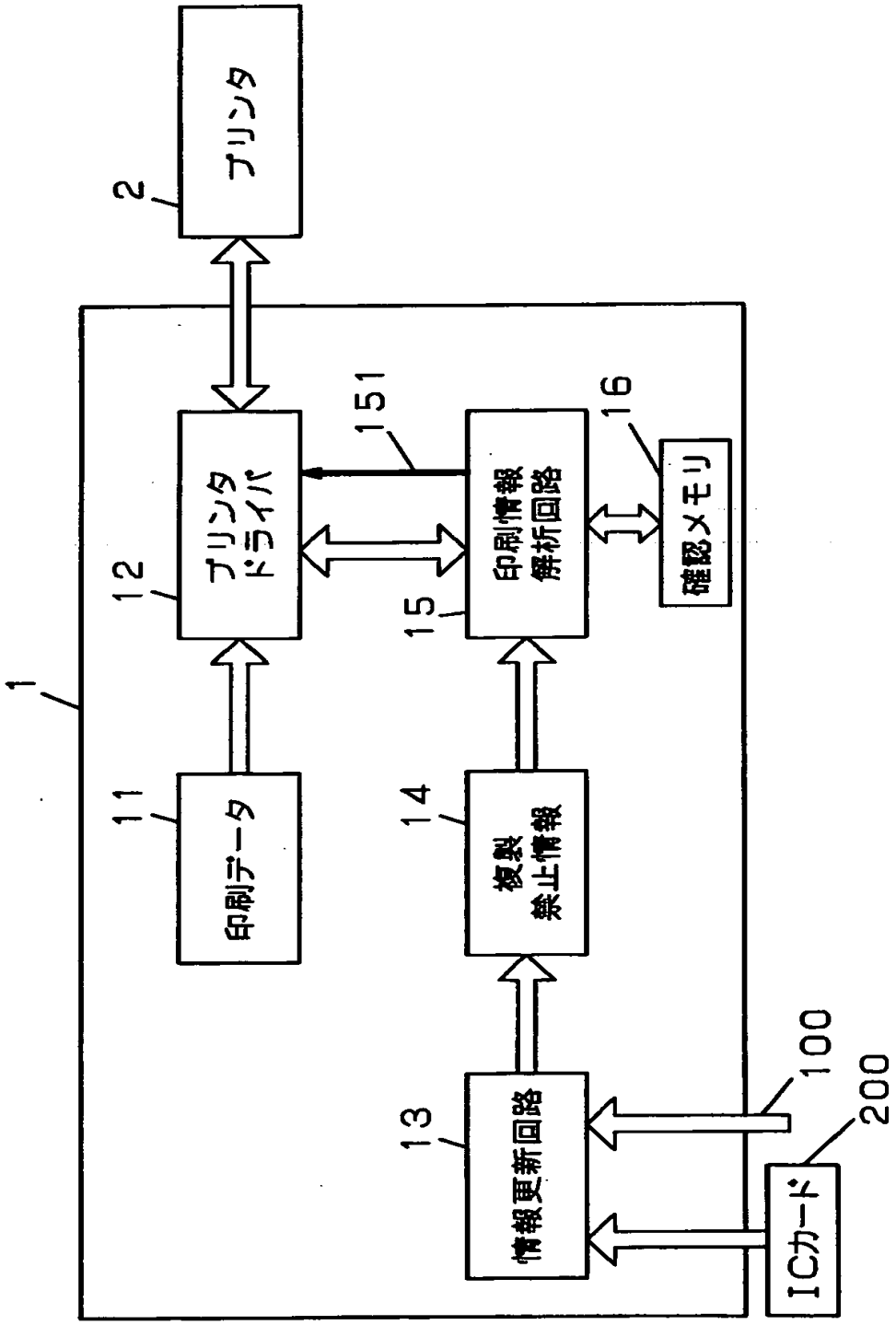
１５０　記録媒体

２００　ＩＣカード

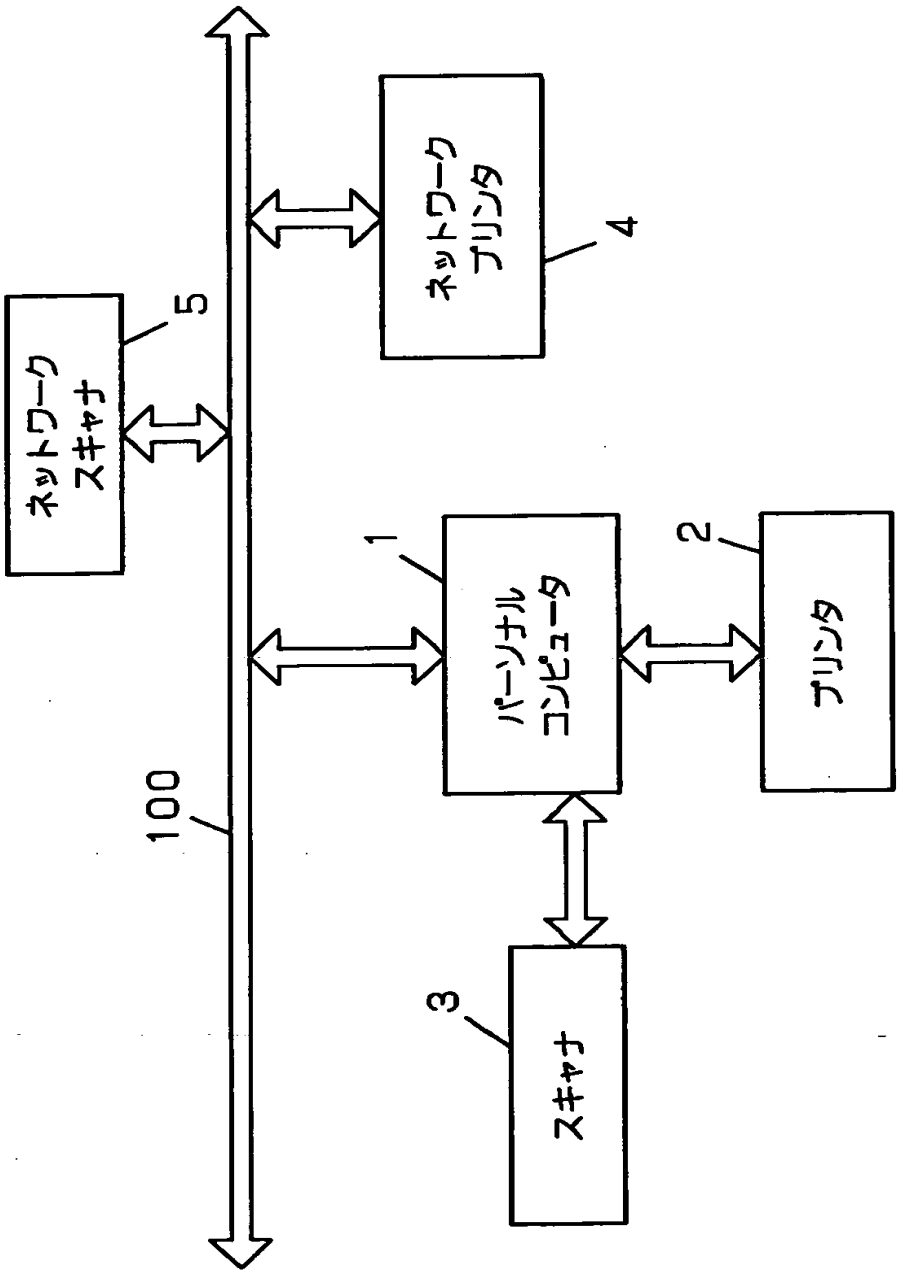
５００　メモリカード

【書類名】　　図面

【図１】

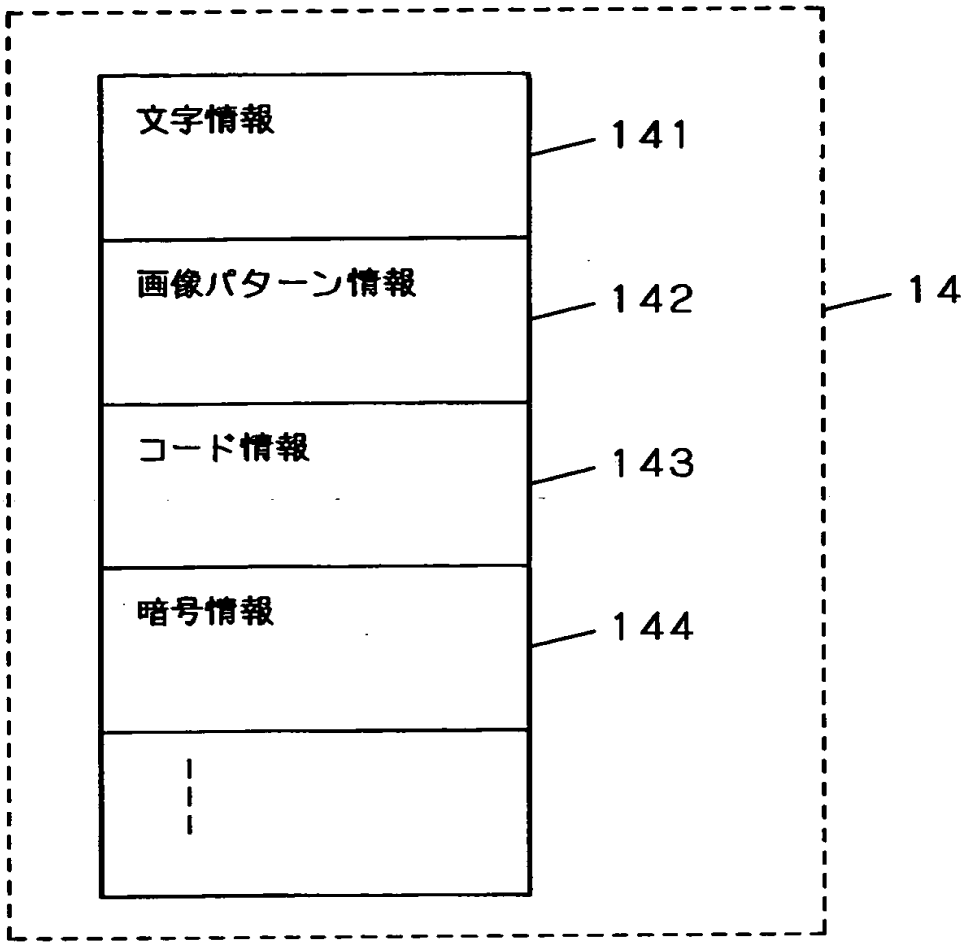

プリンタ
2
プリンタドライバ
12
印刷データ
11
印刷情報解析回路
15
151
16
確認メモリ
複製禁止情報
14
情報更新回路
13
100
200
ICカード
1

【図２】

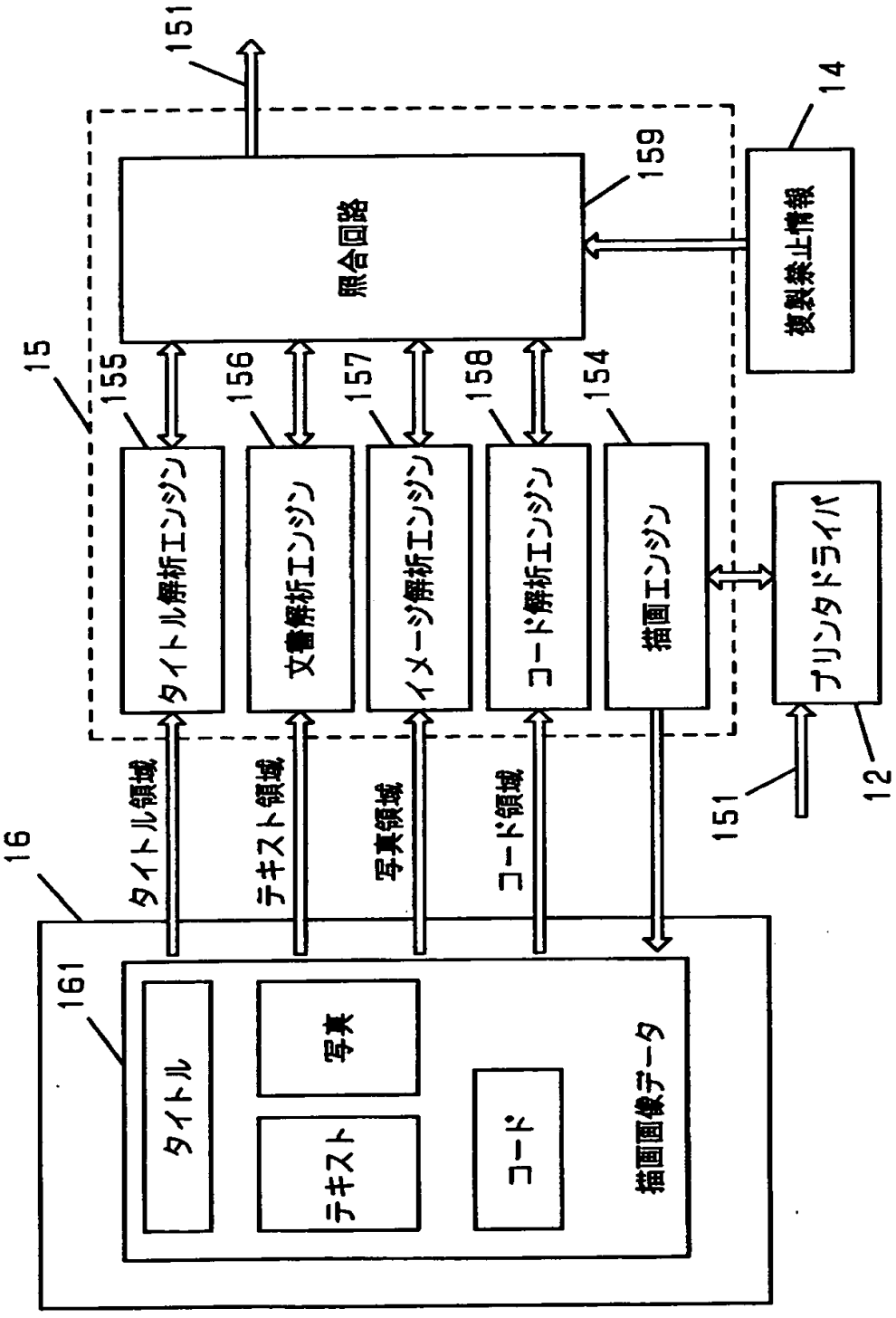


出証特２０００－３０１２８２５

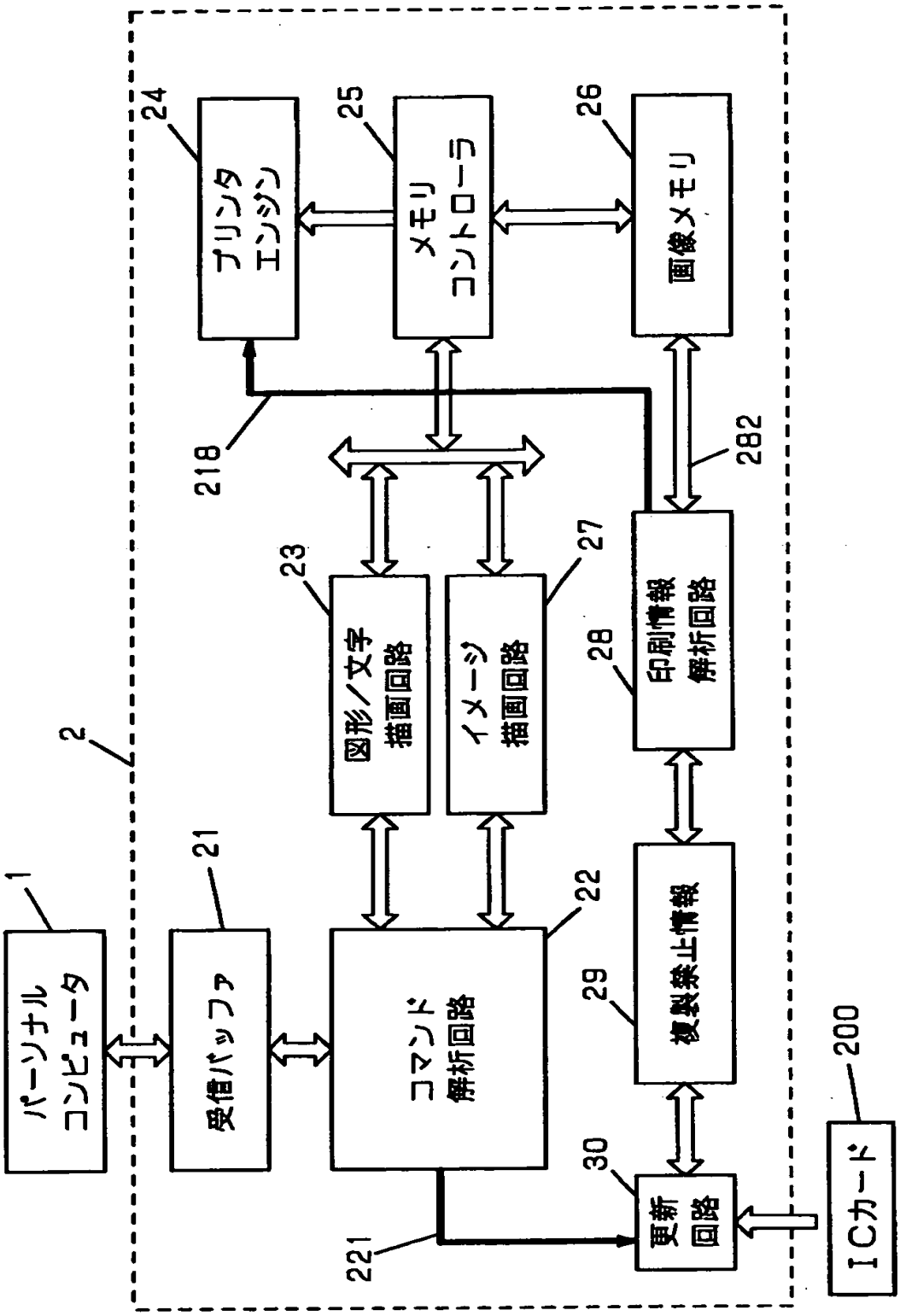
【図３】



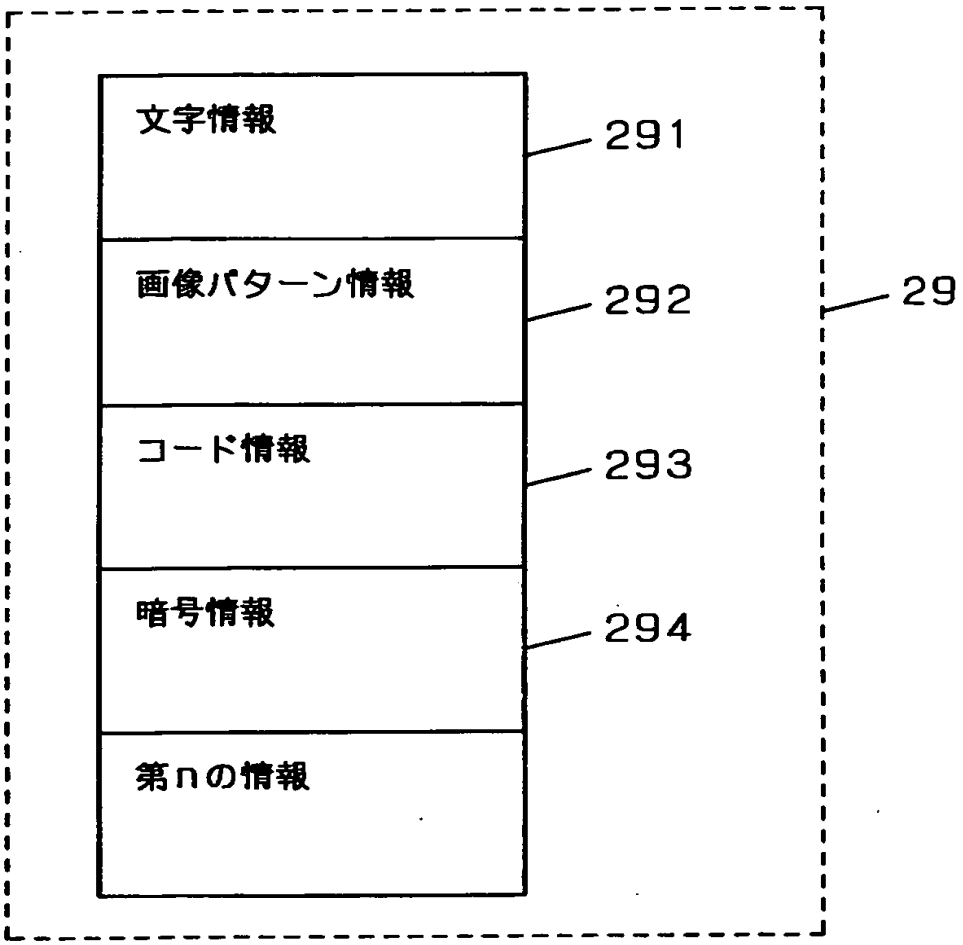
【図４】


151
14
159
照合回路
複製禁止情報
15
155
156
157
158
154
タイトル解析エンジン
文書解析エンジン
イメージ解析エンジン
コード解析エンジン
描画エンジン
プリンタドライバ
タイトル領域
テキスト領域
写真領域
コード領域
151
12
16
161
タイトル
写真
テキスト
コード
描画画像データ

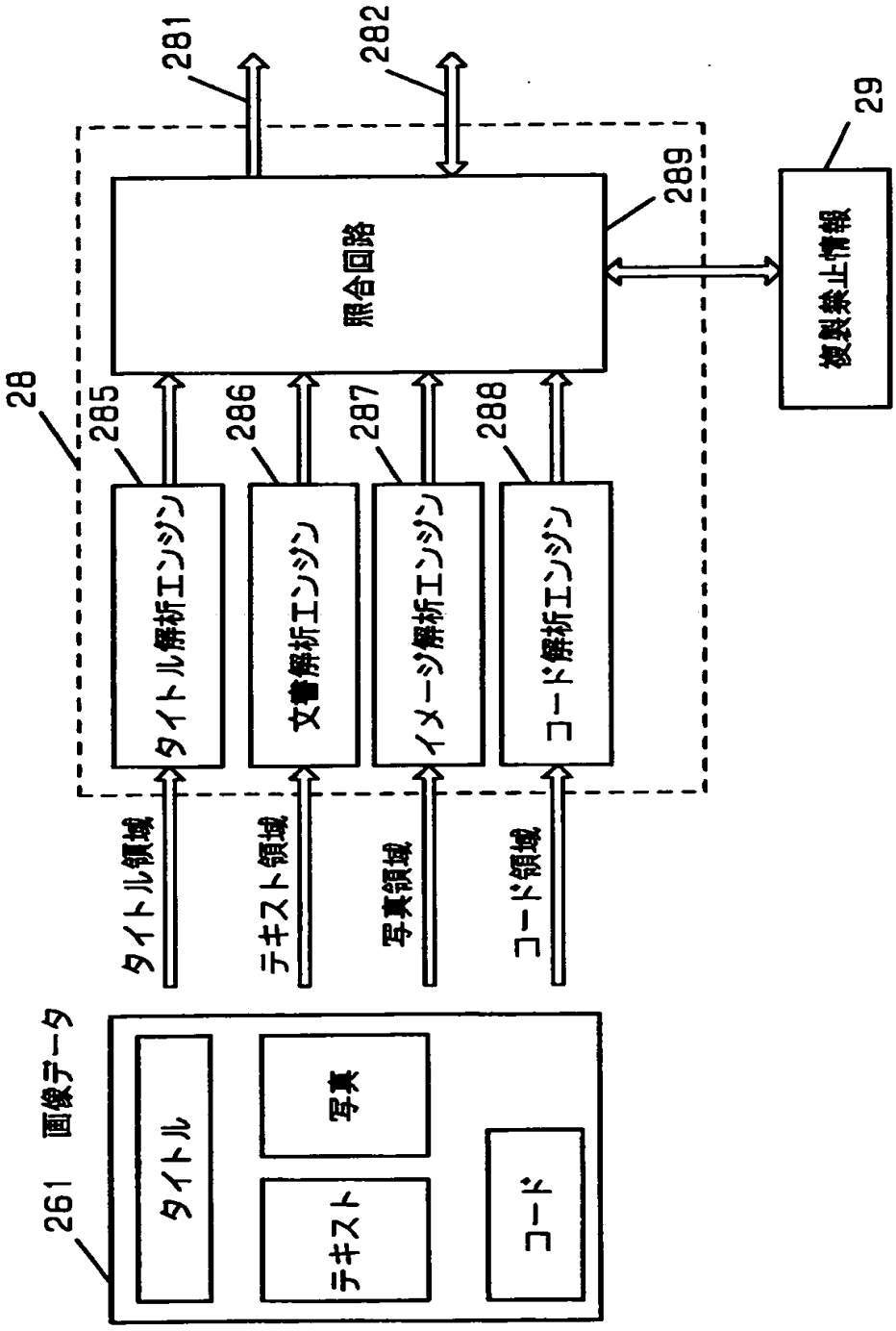
【図５】


パーソナル
コンピュータ
1
2
受信バッファ
21
コマンド
解析回路
22
図形／文字
描画回路
23
プリンタ
エンジン
24
メモリ
コントローラ
25
画像メモリ
26
イメージ
描画回路
27
印刷情報
解析回路
28
複製禁止情報
29
更新
回路
30
ICカード
200
218
282
221

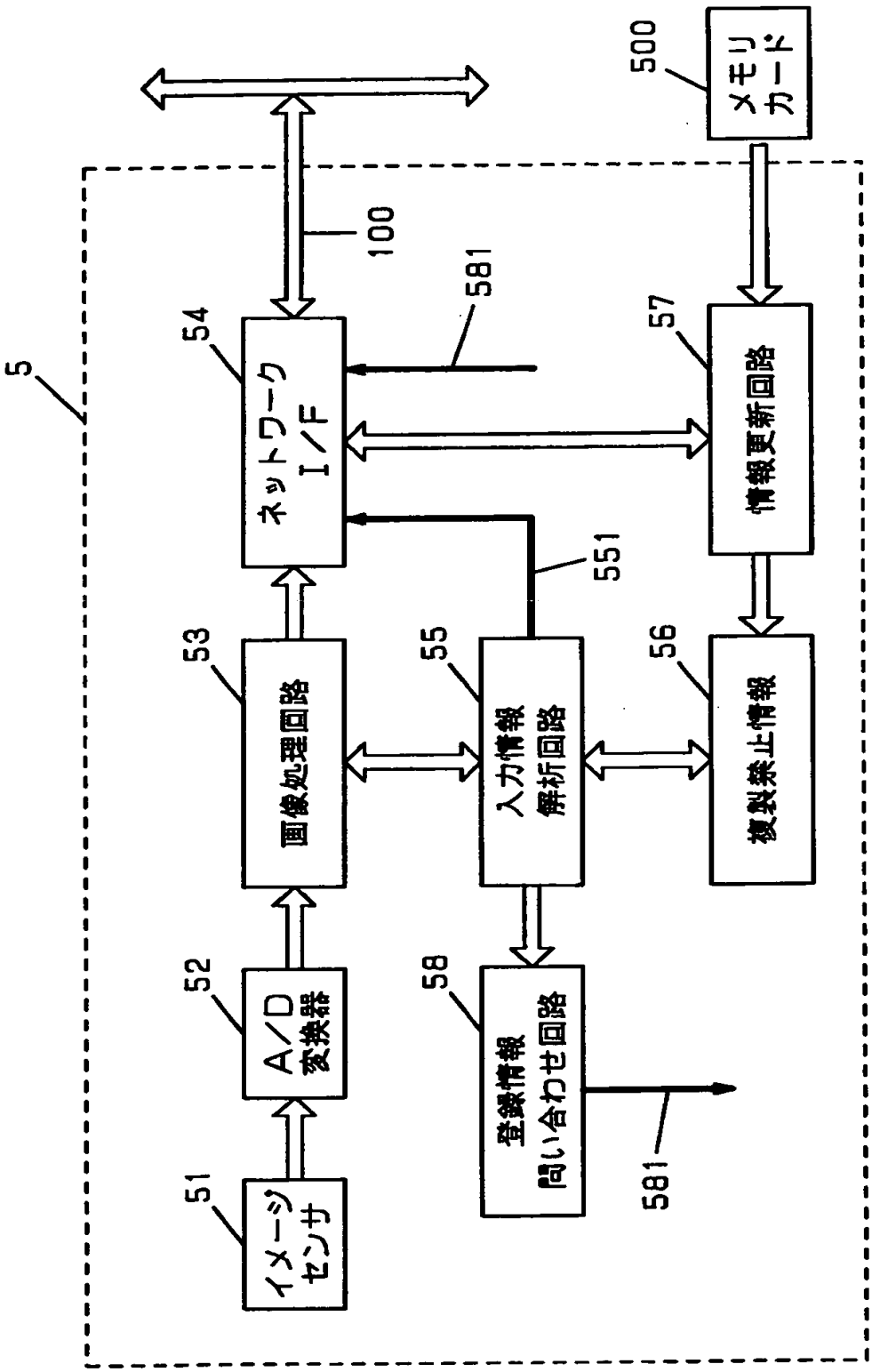
【図６】



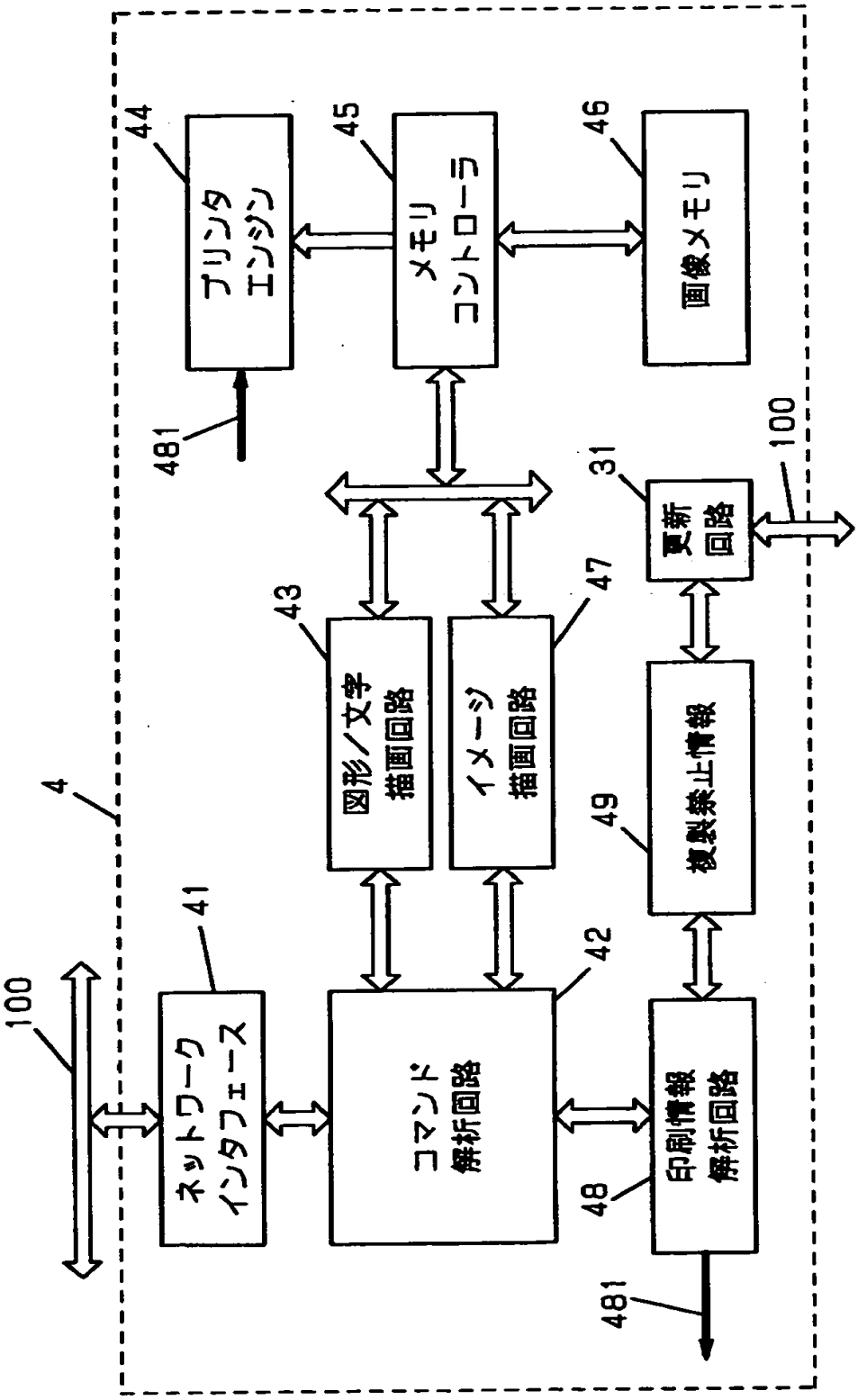
【図７】


281
282
29
289
照合回路
複製禁止情報
28
285
286
287
288
タイトル解析エンジン
文書解析エンジン
イメージ解析エンジン
コード解析エンジン
タイトル領域
テキスト領域
写真領域
コード領域
261 画像データ
タイトル
写真
テキスト
コード

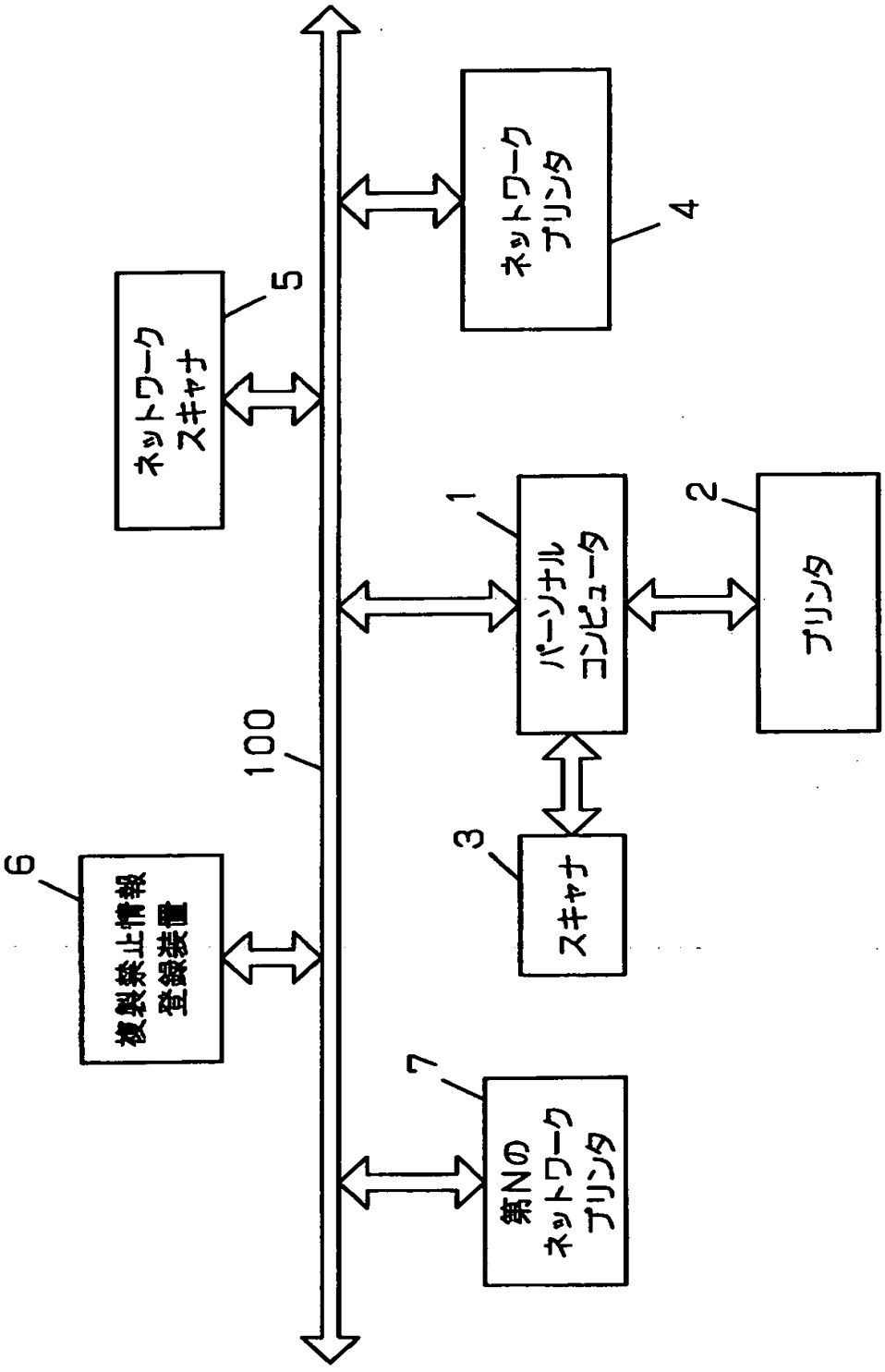
【図８】


500
メモリカード
100
581
5
54
ネットワークI／F
57
情報更新回路
551
53
画像処理回路
55
入力情報解析回路
56
複製禁止情報
52
A／D変換器
58
登録情報問い合わせ回路
581
51
イメージセンサ

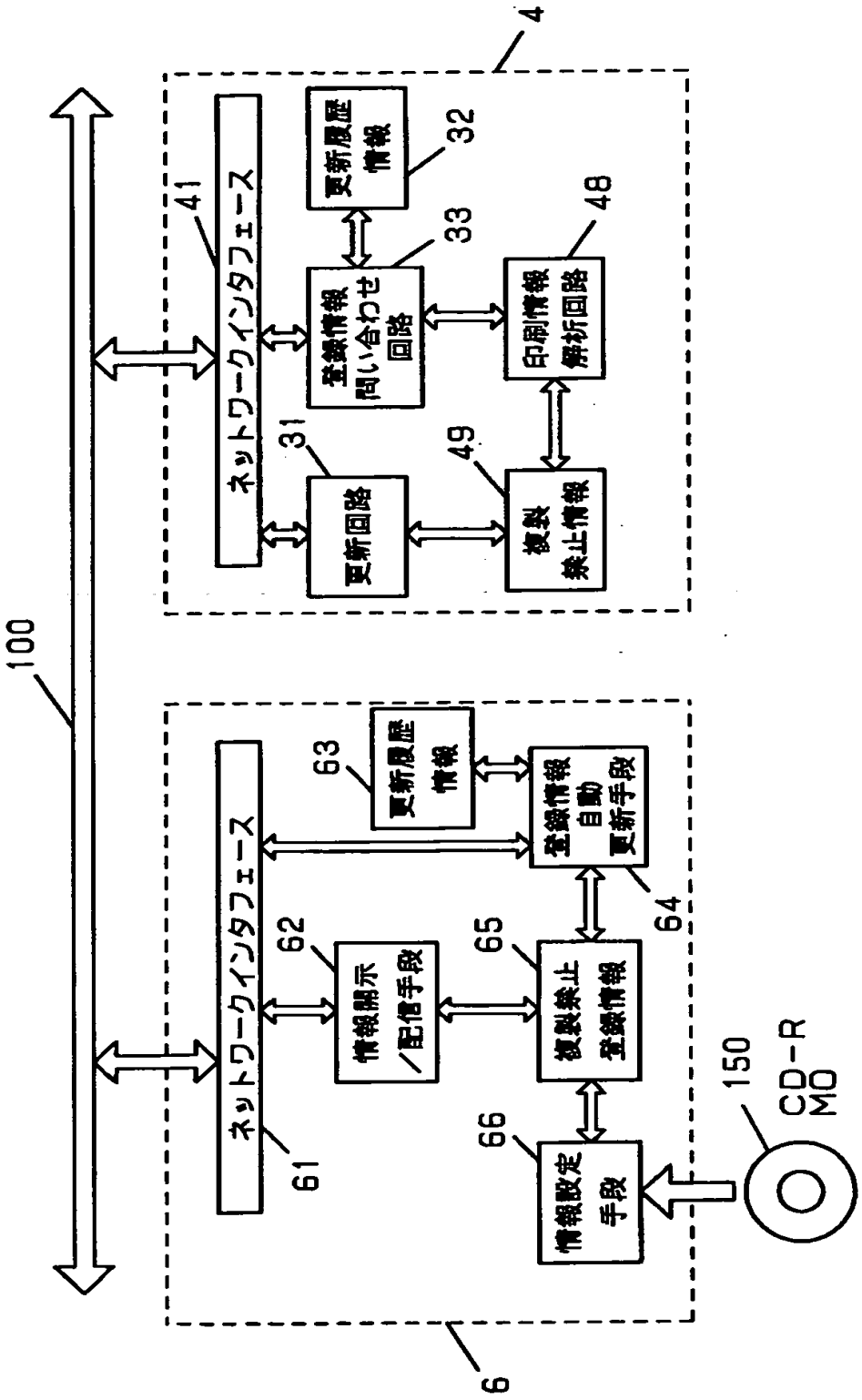
【図９】


4
44
プリンタ
エンジン
45
メモリ
コントローラ
46
画像メモリ
481
31
更新
回路
100
43
図形／文字
描画回路
47
イメージ
描画回路
49
複製禁止情報
41
42
100
ネットワーク
インタフェース
コマンド
解析回路
印刷情報
解析回路
48
481

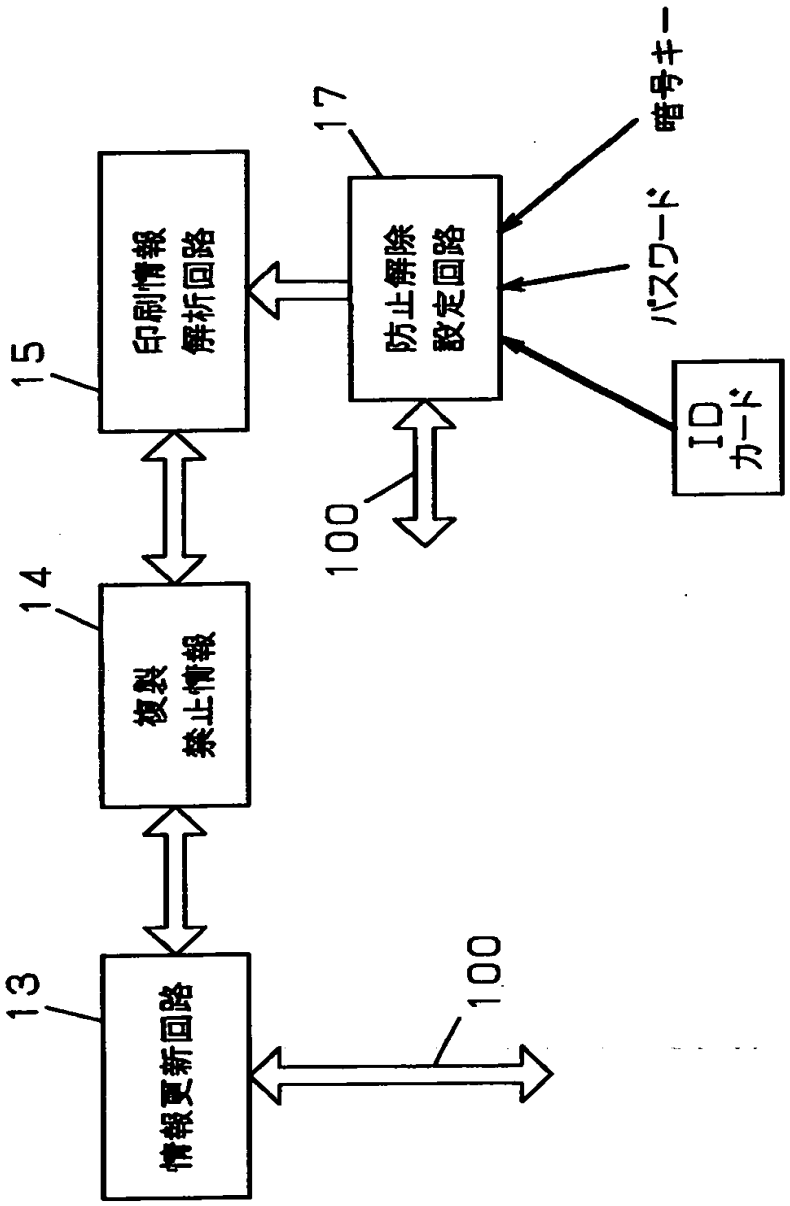
【図１０】


ネットワーク
プリンタ
4
ネットワーク
スキャナ
5
1
パーソナル
コンピュータ
2
プリンタ
100
3
スキャナ
6
複製禁止情報
登録装置
7
第Nの
ネットワーク
プリンタ

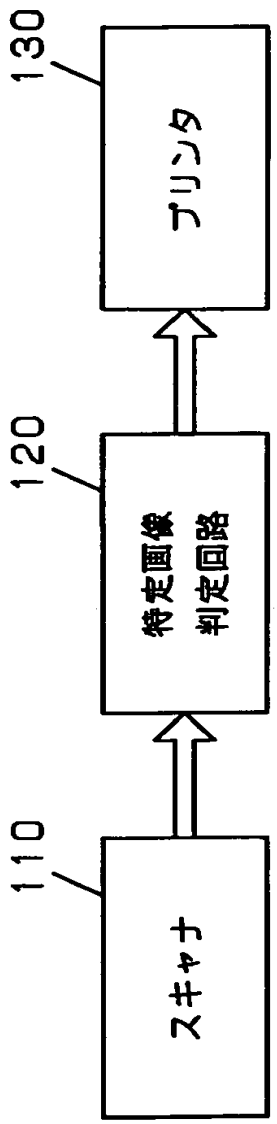
【図１１】


4
更新履歴情報
32
41
ネットワークインタフェース
登録情報問い合わせ回路
33
印刷情報解析回路
48
31
更新回路
49
複製禁止情報
100
63
更新履歴情報
登録情報自動更新手段
64
62
情報開示/配信手段
65
複製禁止登録情報
ネットワークインタフェース
61
66
情報設定手段
150
CD-R
MO
6

【図１２】


17
暗号キー
パスワード
IDカード
防止解除設定回路
印刷情報解析回路
15
14
複製禁止情報
100
13
情報更新回路
100

【図１３】



【書類名】　要約書

【要約】

【課題】　迅速に、不正な複製を未然に防ぐことができるデータ監視方法。

【解決手段】　パーソナルコンピュータ１からプリンタ２にプリンタドライバ１２を経由して印刷データ１１を転送する際、印刷情報解析回路１５が印刷データ１１をモニターし、確認メモリ１６で展開像を確認しながら、複製禁止情報１４からの情報と照合および解析を行なう。もし、この印刷データ１１の展開像が予め複製禁止情報１４に登録されているものと判定した場合は、プリンタドライバ１２に指示してプリンタ２への印刷データの転送を停止させる。これによって、不正な複製データをプリンタ２に出力する前に防止する。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
　〔変更理由〕　新規登録
　　住　所　　大阪府門真市大字門真１００６番地
　　氏　名　　松下電器産業株式会社